ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE ADMINISTRACIÓN DE EMPRESAS

ESCUELA DE CONTABILIDAD Y AUDITORÍA

INGENIERÍA EN CONTABILIDAD Y AUDITORÍA CPA.

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA.

TEMA:

AUDITORÍA INFORMÁTICA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN EN LA DIRECCIÓN PROVINCIAL DEL AMBIENTE DE PASTAZA, PERÍODO 2013.

CAJAMARCA LEMA CÉSAR MAURICIO

RIOBAMBA - ECUADOR

2015

CERTIFICACIÓN DEL TRIBUNAL

Certificamos que el presente trabajo de investigación sobre el tema "AUDITORÍA INFORMÁTICA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN EN LA DIRECCIÓN PROVINCIAL DEL AMBIENTE DE PASTAZA, PERÍODO 2013." previo a la obtención del título de Ingeniero en Contabilidad y Auditoría C.P.A., ha sido desarrollado por el Sr. CAJAMARCA LEMA CÉSAR MAURICIO, ha cumplido con las normas de investigación científica y una vez analizado su contenido, se Autoriza su presentación.

Para constancia firman.

Lic. Iván Patricio Arias González	Ing. Hítalo Bolívar Veloz Segovia
DIRECTOR	**MIEMBRO DE TRIBUNAL**

CERTIFICADO DE RESPONSABILIDAD

Yo, **CAJAMARCA LEMA CÉSAR MAURICIO,** estudiante de la Escuela de Ingeniería en Contabilidad y Auditoría de la Facultad de Administración de Empresas, declaro que la tesis que presento es auténtica y original. Soy responsable de las ideas expuestas y los derechos de Autoría corresponden a la Escuela Superior Politécnica de Chimborazo.

_____

Cajamarca Lema César Mauricio
AUTOR

DEDICATORIA

.

Es muy grato dedicar esta investigación en primera instancia a Dios por darme la maravillosa oportunidad de vida y cumplir con mis metas y objetivos.

A mi Madre y Hermanos, quienes han sido testigos y el pilar fundamental para mi formación profesional.

A mi Esposa e Hija quienes han sido fuente de motivación e inspiración en los momentos más difíciles de mi vida; y, a todos quienes de una u otra manera han contribuido para la realización y culminación de este trabajo.

MAURICIO CAJAMARCA L.

AGRADECIMIENTO

Mi sincero agradecimiento a la Escuela superior Politécnica de Chimborazo, a la Facultad de Administración de Empresas y muy particularmente a la Escuela de Contabilidad y Auditoría y su planta decente por inculcarme valores, principios y conocimientos necesarios para una formación tanto profesional como personal.

Al Lic. Iván Arias e Hítalo Veloz, quienes con las suficientes y oportunas tutorías lograron dirigir con éxito este trabajo investigativo.

A todos y cada uno de los funcionarios quienes conforman la Dirección Provincial del MAE-PASTAZA, por permitirme acceder a la información necesaria para poder realizar el presente trabajo.

MAURICIO CAJAMARCA L.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN EJECUTIVO

La presente investigación es una "Auditoría Informática de las Tecnologías de Información y Comunicación en la Dirección Provincial del Ambiente de Pastaza, período 2013**.**". Con el objetivo de establecer el nivel de cumplimiento de las Normas de Control Interno emitidas por la Contraloría General del Estado, grupo 400 y sub grupo 410 que respecta a *"TECNOLOGÍA DE INFORMACIÓN".*

Previamente a la realización de la Auditoría se analizó la estructura de la organización, puntualmente la unidad de Tecnologías, en cuanto a procesos, planes, y objetivos que garantice el buen uso, manejo, administración y gestión del recurso tecnológico.

Esta Auditoría consta de tres etapas: en la primera etapa se dan los lineamientos para la planeación de la Auditoría, se conoce la operatividad del Área Informática, dando así el inicio a la Auditoría; en la segunda etapa se ejecuta la Auditoría para determinar y analizar el cumplimiento de normas referentes a la seguridad lógica, seguridad física, uso y administración del recurso tecnológico; en la tercera etapa se exponen las falencias encontradas en cuanto a la aplicación de normas establecidas, por lo que se emite un informe de Auditoría Informática con conclusiones y recomendaciones.

Esta investigación surge para evidenciar errores y/o falencias en el manejo de los recursos tecnológicos, que comprometan la integridad de datos, información e infraestructura tecnológica.

Se recomienda a los funcionarios del MAE-PASTAZA la puesta en ejecución de las conclusiones y recomendaciones planteadas en el informe de Auditoría Informática.

_____

Lic. Iván Patricio Arias González
DIRECTOR

SUMMARY

The current research work is an "Informatics Audit of the Information and Communication Technologies at the Environmental Provincial Department from Pastaza, 2013 period." Which aims to rate the level of fulfillment of the Internal Control regulations stated by the General Comptroller of the State, group 400 and sub group 410 related to "INFORMATION TECHNOLOGIES".

Previous to the Audit application, the organizational structure was analyzed, specifically the Technologies unit, concerning to processes, plans and objectives which guarantee the proper use, handling, administration and management of the technological resource.

This Audit is made up of three stages: on the first stage, the outline for the Audit planning is provided; the operability of the Informatics Area is known in order to start with the Audit. On the second stage the Audit is carried on in order to determine and analyze the fulfillment of the regulations related to logics security, physical security, use and administration of the technological resource; on the third stage, the failures found are displayed regarding to the application of the stated regulations, for instance, an Informatics Audit report is delivered with its corresponding conclusions and recommendations.

This research work comes out t evidence mistakes and/or failures upon the management of technological resources which risks the integrity of data, information and technological infrastructure.

It is recommended to the personnel of MAE-PASTAZA, the execution of the conclusions and recommendations stated in the report of the Informatics Audit.

INTRODUCCIÓN

La Dirección Provincial del MAE-PASTAZA, en concordancia con lo decretado en la Constitución Política de la República del Ecuador de 2008, vela por un ambiente sano y el respeto a la naturaleza.

Para la realización de una gestión ambiental eficaz y eficiente es de suma importancia contar con una Unidad Tecnológica, con la suficiente autonomía e independencia ajustada a la necesidad de esta dirección, de tal modo que salvaguarde los sistemas de información y por ende la integridad de la información que contienen dichos equipos.

El manejo de las Tecnologías de Información y Comunicación de la Dirección Provincial del MAE-PASTAZA enfrenta falencias en los diferentes procesos y políticas de uso, manejo, gestión y administración de dicha unidad, dando paso así, al incumpliendo de normas y leyes establecidas para el buen manejo de estos recursos.

Por todo lo mencionado se procede a ejecutar una Auditoría Informática a la dirección provincial del MAE-PASTAZA con el fin de obtener un informe de auditoría con sus respectivas conclusiones y recomendación que guíen a los funcionarios de la institución a una adecuada toma de decisiones que ayuden al desarrollo de la unidad informática de la institución.

CAPÍTULO I: PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La Dirección Provincial del Ambiente Pastaza, en concordancia con lo decretado en la Constitución Política de la República del Ecuador de 2008, vela por un ambiente sano y el respeto a la naturaleza. Garantizará un modelo sustentable de desarrollo ambientalmente equilibrado y respetuoso de la diversidad cultural, que conserve la biodiversidad y la capacidad de regeneración natural de los ecosistemas, y asegure la satisfacción de las necesidades de las generaciones presentes y futuras.

Para la realización de una gestión ambiental eficaz y eficiente es de suma importancia contar con una Unidad Tecnológica, con la suficiente autonomía e independencia ajustada a la necesidad de esta dirección, de tal modo que salvaguarde los sistemas de información y comunicación, disminuya gastos, agilite y reduzca trámites, etc. y así lograr ejercer una rectoría de la gestión ambiental que asegure el buen manejo de los recursos naturales de la provincia.

El manejo de las Tecnologías de Información y Comunicación de la Dirección Provincial del ambiente Pastaza enfrenta vacíos en los diferentes procesos, delimitando funciones y autonomía de dicha unidad, dando paso así, al incumpliendo de normas y leyes establecidas para el buen manejo de estos recursos. Un problema latente de la institución en esta unidad se da en la autonomía y estructura que debe tener debido a que el manejo, otorgamiento, desbloqueo y la gestión en sí de los accesos a los equipos Informáticos de esta dirección se debe notificar a la Dirección Nacional del Ministerio del Ambiente situado en la ciudad de Quito y así poder suplir a estas necesidades, así como también en los procesos de adquisición, mantenimiento y soporte técnico se debe proceder de la misma manera.

Todo esto hace que la Dirección Provincial del ambiente Pastaza este incumpliendo con normas y leyes establecidas para el buen manejo, administración y uso de las tecnologías de Información y Comunicación.

1.1.1 Formulación del problema

¿Cómo una Auditoria Informática de las Tecnologías de Información y Comunicación en la Dirección Provincial del ambiente de Pastaza, período 2013, permitirá el cumplimiento de normas y leyes establecidas?

1.1.2 Delimitación del problema

Campo: Auditoría Informática

Área: Tecnologías de Información y Comunicación

Temporal: Periodo 2013

Espacial: Dirección Provincial del ambiente de Pastaza

1.2 OBJETIVOS

1.2.1. Objetivo General

Realizar una Auditoría Informática de las Tecnologías de Información y Comunicación en la Dirección Provincial del Ambiente de Pastaza, período 2013", para establecer en nivel de cumplimiento de normas y leyes establecidas.

1.2.2 Objetivos Específicos

- ✓ Evaluar la administración, manejo y uso de las Tecnologías de Información y comunicación, para determinar el grado de cumplimiento de leyes y normas establecidas.

- ✓ Aplicar métodos y técnicas previstas para la Auditoria Informática que se ajusten a las necesidades de la institución, para obtener un resultado eficiente y eficaz.

- ✓ Emitir un informe con Comentarios, Conclusiones y Recomendaciones para un buen manejo de las Tecnologías de Información y Comunicación, así como también a la toma de decisiones y acciones correctivas si así lo fuere necesario.

1.3 JUSTIFICACIÓN DE LA INVESTIGACIÓN

La Auditoria Informática puede evidenciar posibles errores y/o falencias en el manejo de los recursos tecnológicos de la Dirección Provincial del Ambiente Pastaza. En primera instancia se ha notado una gran carencia de un departamento o unidad informática que funcione con total independencia y autonomía dentro de la institución, todo esto acarrea a problemas secundarios como una ineficaz administración, no se evidencia que se defina y se delimite funciones, así como también la falta de políticas y procedimientos para un adecuado manejo de este recurso. La inexistencia de esta unidad origina también como resultado, una mala asistencia técnica a la hora de salvaguardar la información porque carece de procesos de seguridad informática que precautelen íntegramente la información. Otro punto desfavorable es que los funcionarios y usuarios de las tecnologías de información y comunicación no están capacitados para garantizar un correcto manejo de este recurso de la institución.

Todos estos problemas se presentan principalmente por la inadecuada aplicación de normas y leyes (Normas de Control Interno emitidas por la Contraloría General del Estado) establecidas para una buena administración, uso y manejo del recurso tecnológico, que salvaguardan y garantizan confiabilidad, confidencialidad y disponibilidad de la información que posee la entidad.

La aplicación de la Auditoria Informática permitirá corregir estos errores de aplicación e inconsistencias con la norma establecida, para así evitar en un futuro sanciones de parte del órgano regulador y lo que es más importante evitar el deterioro, pérdida total o parcial de la información que posee la entidad para la ejecución de sus funciones, tareas y atención eficiente y eficaz a todos sus usuarios.

Por otra parte esta investigación generará un aporte académico en lo que respecta a la Auditoría Informática, ya que se cuenta con la disponibilidad de información necesaria debidamente documentada otorgada por los funcionarios de la institución según las necesidades y casos que se presente en el desarrollo de la misma.

Finalmente es importante señalar que esta investigación permitirá poner en evidencia los conocimientos adquiridos durante la etapa de aprendizaje, cumpliendo así con un

requisito indispensable y necesario previo a la obtención del título de ingeniería en Contabilidad y Auditoría CPA.

CAPÍTULO II: MARCO TEÓRICO

2.1 GENERALIDADES DE AUDITORÍA INFORMÁTICA

2.1.1 Antecedentes

Al igual que en los la auditoría en general, en la Auditoría Informática también existen antecedentes en el ámbito internacional. Para sustentar esto citamos a los siguientes autores.

Según (Muñoz Raso, 2002, págs. 9-10)

En 1988, Echenique publicó su libro Auditoría de sistemas, en el cual establece las principales bases para el desarrollo de una auditoría de sistemas computacionales, dando un enfoque teórico-práctico sobre el tema.

En 1992, Lee presentó un libro en el cual enuncia los principales aspectos a evaluar en una auditoría de sistemas, mediante una especie de guía que le indica al auditor los aspectos que debe evaluar en este campo.

En 1993, Rosalva Escobedo Valenzuela presenta en la UVM una tesis de auditoría a los centros de cómputo, como apoyo a la gerencia, destacando sus aspectos más importantes.

En 1994, G. Haffes, F. Holguín y A. Galán, en su libro sobre auditoría de los estados financieros, presentan una parte relacionada con la auditoría de sistemas, que profundiza en los aspectos básicos de control de sistemas y se complementa con una serie de preguntas que permiten evaluar aspectos relacionados con este campo.

En 1995, Ma. Guadalupe Buendía Aguilar y Edith Antonieta Campos de la O. presentan un tratado de auditoría informática (apoyándose en lo señalado por el maestro Echenique), en el cual presentan metodologías y cuestionarios útiles para realizar esta especialidad.

En 1995, Yann Darrien presenta un enfoque particular sobre la auditoría de sistemas.

En 1996, Alvin A. Arens y James K. Loebbecke, en su libro Auditoría. Un enfoque integral, de Prentice Hall Hispanoamericana, S. A., nos presentan una parte de esta obra como Auditoría de Sistemas Complejos de PED.

En 1996, Hernández Hernández propone la auditoría en informática, en la cual da ciertos aspectos relacionados con esta disciplina.

En 1997, Francisco Ávila obtiene mención honorífica en su examen profesional, en la UVM, Campus San Rafael, con una tesis en la cual propone un caso práctico de auditoría de sistemas realizado en una empresa paraestatal.

En 1998, Yang Darrien presenta Técnicas de auditoría, donde hace una propuesta de diversas herramientas de esta disciplina.

En 1998, Mario G. Piattini y Emilio del Peso presentan Auditoría informática, un enfoque práctico, donde mencionan diversos enfoques y aplicaciones de esta disciplina.

2.2. FUNDAMENTACIÓN TEÓRICA

2.2.1 Auditoría

2.2.1.1 Definición

Según el Manual Latinoamericano de auditoría profesional en el sector público (ILACI). (2008) menciona que: "Es el examen objetivo, sistemático y profesional de las operaciones financieras o administrativas, efectuado por auditores profesionales con posterioridad a su ejecución con la finalidad de verificarlas, evaluarlas y elaborar el informe que contenga comentarios, conclusiones y recomendaciones; y, en el caso de examen de Estados Financieros, el correspondiente dictamen profesional." **(p. 32)**

(Muñoz Raso, 2002, pág. 34) **menciona que "**Auditoría es la revisión independiente que realiza un auditor profesional, aplicando técnicas, métodos y procedimientos especializados, a fin de evaluar el cumplimiento de las funciones, actividades, tareas y procedimientos de una entidad administrativa, así como dictaminar sobre el resultado de dicha evaluación".

Del análisis de estas definiciones obtenemos el siguiente concepto:

La auditoría es aquella evaluación realizada por un profesional del campo, que se aplica a hechos económicos, administrativos pasados mediante técnicas y procedimientos con el fin de emitir un Informe independiente y Objetivo.

2.2.1.2 Tipos de Auditoría

(Muñoz Raso, 2002, págs. 12-13)**, propone la siguiente clasificación:**

A. Auditorías por su lugar de aplicación

- Auditoría externa
- Auditoría interna

B. Auditorías por su área de aplicación

- Auditoría financiera
- Auditoría administrativa
- Auditoría operacional
- Auditoría integral
- Auditoría gubernamental
- Auditoría de sistemas

C. Auditorías especializadas en áreas específicas

- Auditoría al área médica (evaluación médico-sanitaria)
- Auditoría al desarrollo de obras y construcciones (evaluación de ingeniería)
- Auditoría fiscal
- Auditoría laboral
- Auditoría de proyectos de inversión
- Auditoría a la caja chica o caja mayor (arqueos)
- Auditoría al manejo de mercancías (inventarios)
- Auditoría ambiental
- Auditoría de sistemas

D. Auditoría de sistemas computacionales

- Auditoría informática

- Auditoría con la computadora
- Auditoría sin la computadora
- Auditoría a la gestión informática
- Auditoría al sistema de cómputo
- Auditoría alrededor de la computadora
- Auditoría de la seguridad de sistemas computacionales
- Auditoría a los sistemas de redes
- Auditoría integral a los centros de cómputo
- Auditoría ISO-9000 a los sistemas computacionales
- Auditoría outsourcing
- Auditoría ergonómica de sistemas computacionales

2.2.2 Auditoría Informática

2.2.2.1 Definiciones

Según Echenique, J. (2009) manifiesta que "es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá papa la adecuada toma de decisiones" **(p. 18).**

(Piattini & Del Poso, 2008, pág. 7)**, manifiestan que "**La Auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficaz mente los recursos".

Según (Muñoz Raso, 2002, págs. 23-24)**, manifiesta que:**

Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y de más componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumos necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto

ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas informáticos a la empresa.

Analizando estas definiciones se puede determinar el siguiente concepto:

La auditoría Informática es aquella que se encarga de evaluar la Administración, manejo y uso de las Tecnologías de Información con el fin de salvaguardar íntegramente los datos e información de la empresa.

2.2.2.2 Importancia de Auditoria Informática

(Carchi, 2013)**, expone:**

La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

2.2.2.3 Objetivos de la auditoria informática

Según (Muñoz Raso, 2002, págs. 39-40) **manifiesta que:**

La evaluación a los sistemas computacionales, a la administración al centro de cómputo, al desarrollo de proyectos informáticos, a la seguridad de los sistemas computacionales y a todo lo relacionado con ellos, será considerada bajo los siguientes objetivos:

- Realizar una evaluación con personal multidisciplinario y capacitado en el área de sistemas, con el fin de emitir un dictamen independiente sobre la razonabilidad de las operaciones del sistema y la gestión administrativa del área de informática.
- Hacer una evaluación sobre el uso de los recursos financieros en las áreas del centro de información, así como del aprovechamiento del sistema computacional, sus equipos periféricos e instalaciones.

- Evaluar el uso y aprovechamiento de los equipos de cómputo, sus periféricos, las instalaciones y mobiliario del centro de cómputo, así como el uso de sus recursos técnicos y materiales para el procesamiento de información.
- Evaluar el aprovechamiento de los sistemas de procesamiento, sus sistemas operativos, los lenguajes, programas y paqueterías de aplicación y desarrollo, así como el desarrollo e instalación de nuevos sistemas.
- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas y lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de los usuarios del centro de información.
- Realizar la evaluación de las áreas, actividades y funciones de una empresa, contando con el apoyo de los sistemas computacionales, de los programas especiales para auditoría y de la paquetería que sirve de soporte para el desarrollo de auditorías por medio de la computadora.

2.2.2.4 Metodología para la ejecución de la Auditoría Informática

Tabla 1: Etapas de Auditoría

1ª etapa	**Planeación de la auditoría de sistemas computacionales**
	• Identificar el origen de la auditoría. • Realizar una visita preliminar al área que será evaluada. • Establecer los objetivos de la auditoría. • Determinar los puntos que serán evaluados en la auditoría. • Elaborar planes, programas y presupuestos para realizar la auditoría. • Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría. • Asignar los recursos y sistemas computacionales para la auditoría
2ª etapa	**Ejecución de la auditoría de sistemas computacionales**
	• Realizar las acciones programadas para la auditoría. • Aplicar los instrumentos y herramientas para la auditoría.

	• Identificar y elaborar los documentos de desviaciones encontradas. • Elaborar el dictamen preliminar y presentarlo a discusión. • Integrar el legajo de papeles de trabajo de la auditoría.
3ª etapa	**Dictamen de la auditoría de sistemas computacionales**
	• Analizar la información y elaborar un informe de situaciones detectadas • Elaborar el dictamen final. • Presentar el informe de auditoría.

Fuente: (Muñoz, C. (2002) p. 185)
Elaborado por: César Mauricio Cajamarca Lema

2.2.2.5 Informe de Auditoría Informática

(Muñoz Raso, 2002, pág. 280)**, atribuye que:**

En la redacción del informe, el auditor señala los resultados de su investigación, sus evaluaciones, hallazgos, aportaciones y conclusiones sobre el trabajo realizado; también señala las técnicas, herramientas, métodos y procedimientos que utilizó en la obtención de datos, las observaciones, interpretaciones de los fenómenos y hechos evaluados que le sirvieron de sustento en la elaboración del documento de situaciones encontradas o relevantes que informa, así como todas las demás aportaciones con las cuales da su sello personal al informe presentado.

Tomando como base lo que el autor menciona se determina que:

El informe de auditoría Informática es el resultado del trabajo investigativo realizado por el auditor, es donde plasma sus conclusiones y recomendaciones en función de los problemas detectados a lo largo de su trabajo.

2.2.3 Control Interno

2.2.3.1 Definición

Según (Muñoz Raso, 2002, pág. 105)**, manifiesta que**, "El control interno es la adopción de una serie de medidas que se establecen en las empresas, con el propósito de contar con instrumentos tendientes a salvaguardar la integridad de los bienes

institucionales y así ayudar a la administración y cumplimiento correctos de las actividades y operaciones de las empresas.”

De esta definición se puede concluir el siguiente concepto:

El control interno es el marco de referencia y/o normativo que establece el accionar de cada uno de los directivos, trabajadores, funcionarios, etc. de la empresa, el mismo que ayudara a la consecución de las metas y objetivos trazados.

2.2.3.2 Objetivos del Control Interno

(Muñoz Raso, 2002)**, determina lo siguiente:**

Tomando en cuenta que el control interno busca contribuir en la seguridad y protección de los bienes de la empresa, en la obtención de información correcta y oportuna, en la promoción de la eficacia de la operación y en la dirección adecuada de la empresa, se puede establecer que su principal prioridad es la ayuda que proporciona al buen funcionamiento de la institución y a la salvaguarda de su patrimonio. Sin embargo, hace falta una información adecuada para comprobar si se satisfacen esas prioridades.

Además, el control interno también sirve para evaluar el desarrollo correcto de las actividades de las empresas, así como la aceptación y cumplimiento adecuados de las normas y políticas que regulan sus actividades.

Con base en lo anterior, se pueden establecer los siguientes puntos como los objetivos fundamentales del control interno:

- Establecer la seguridad y protección de los activos de la empresa.
- Promover la confiabilidad, oportunidad y veracidad de los registros contables, así como de la emisión de la información financiera de la empresa.
- Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa.
- Establecer y hacer cumplir las normas, políticas y procedimientos que regulan las actividades de la empresa.
- Implantar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades, tareas y funciones de la empresa.

2.2.3.3 Componentes del Control Interno

A. Ambiente de control

Según (Mantilla, 2008, pág. 25)**, manifiesta que** "El ambiente de control tiene una influencia profunda en la manera como se estructuran las actividades del negocio, se establecen los objetivos y se valoran los riesgos…Este componente influye en la conciencia de control de su gente. Las entidades efectivamente controladas se esfuerzan por tener gente competente, inculcan actitudes de integridad y conciencia de control a todo lo ancho de la empresa, y establecen un tono por lo alto positivo."

B. Valoración del riesgo

Según (Estupiñan Gaitán, 2006, pág. 28)**, menciona que** "En toda entidad, es indispensable el establecimiento de objetivos tanto globales de la organización como de actividades relevantes, obteniendo con ello una base sobre la cual sean identificados y analizados los factores de riesgo que amenazan su oportuno cumplimiento".

C. Actividades de control

Según (Mantilla, 2008, pág. 59)**, menciona que** "Las actividades de control se dan a lo largo y ancho de la entidad, en todos los niveles y en todas las funciones, que incluyen: aprobaciones, autorizaciones, verificaciones, reconciliaciones, inspecciones, revisión del desempeño de operaciones, seguridad de activos y segregación de responsabilidades".

D. La información y comunicación

Según (Mantilla, 2008, pág. 71)**, menciona que** "Cada empresa debe capturar información pertinente, financiera y no financiera, relacionada con actividades y eventos tanto externos como internos."

E. Actividades de monitoreo o supervisión

Según el SAS 78 lo define como "La vigilancia es un proceso que asegura la calidad del control interno sobre el tiempo".

2.2.4 Papeles de Trabajo

Según (Franklin, 2007, pág. 620)**, manifiesta que, "**Son registros que conserva el auditor sobre los procedimientos aplicados, las pruebas realizadas, la información obtenida y las conclusiones incluidas en su resumen."

(Farinango Alvear, 2012, pág. 65)**, expone que los papeles de trabajo son,** "El conjunto de cédulas, documentos y medios magnéticos (tendencias a la auditoría cero papeles) elaborados u obtenidos por el auditor, producto de la aplicación de las técnicas, procedimientos y más prácticas de auditoría, que sirven de evidencia del trabajo realizado y de los resultados de auditoría relevados en el informe."

Lo mencionado por estos dos autores se concluye:

Son documentos obtenidos y levantados por el auditor conforme avanza su trabajo y que serán de vital importancia para respaldar sus decisiones finales.

2.2.4.1 Archivo de papeles de trabajo

Los papeles de trabajo se ordenan y referencian de acuerdo con un índice preestablecido que facilite su identificación y lectura durante el curso del examen y posteriormente a este. Debe evitarse archivos individuales que sean voluminosos o difíciles de manejar, los papeles de trabajo son confidenciales y deben guardarse con sumo cuidado en todo momento y bajo condiciones de seguridad.

Los papeles de trabajo se clasifican en:

Archivo corriente: El archivo corriente está conformado por los legajos de papeles de trabajo, que solo tienen validez y constituyen soporte de un período o ejercicio en particular.

Archivo permanente: Este archivo se organiza para cada empresa sujeta a auditoría o entidad a ser controlada, un archivo permanente que contenga información utilizable en futuras auditoría o exámenes especiales.

El objetivo del archivo permanente es facilitar a los auditores información básica sobre la entidad para que se pueda entender con facilidad sus sistemas y esté en condiciones de hacer referencias a documentos que son relevantes cada año, en consecuencia el archivo permanente debe mantenerse actualizado en tanto se continúe realizando la

auditoría a esa empresa, organismo o proyecto, evitando la acumulación de documentos innecesarios.

2.2.5 Marcas de Auditoria

(Muñoz Raso, 2002, pág. 263)**, menciona que "**Son las marcas de carácter informal que utiliza exclusivamente el auditor o el grupo de auditores que realizan la auditoría, con el fin de facilitar la uniformidad de los papeles de trabajo y para identificarlos mejor". **(p. 263)**

Del análisis de la definición se determina:

Son marcas, sellos y abreviaturas que ha de utilizar el auditor para facilitar la clasificación e identificación las acciones tomadas por el mismo.

Tabla 2: Propuesta de símbolos convencionales utilizados en una auditoría Informática

MARCA	SIGNIFICADO/INTERPRETACIÓN
√	Verificado una vez
√	Verificado dos veces
√√	Dato Correcto
X	Dato con error
N/A	No aplica
≠	Diferencias Detectadas
A	Archivo verificado
OBS	Observación
ENT	Entrevista
EF	Entrevista Funcionario
EP	Entrevista al Personal
CUES	Cuestionario

Fuente: (Muñoz, C. (2002) p. 264)
Elaborado por: César Mauricio Cajamarca Lema

2.2.6 Evidencia de la auditoría

(Franklin, 2013, pág. 90)**, menciona que**:

La evidencia representa la comprobación fehaciente de los hallazgos durante el ejercicio de auditoría, por lo que constituye un elemento relevante para fundamentar los juicios y

conclusiones que formula el auditor. Por tal motivo, al reunirlas es preciso prever el nivel de riesgo, incertidumbre y conflicto que pudiera suscitar, así como el grado de confiabilidad, calidad y utilidad real intrínsecos a ella; en consecuencia, es indispensable que el auditor se apegue en todo momento a la línea de trabajo acordada, a las normas en la materia y a los criterios que surjan durante el proceso de ejecución.

La evidencia se puede clasificar en los siguientes rubros:

- **Física**

Se obtiene mediante inspección u observación directa de las actividades, bienes o sucesos, y se presenta por medio de notas, fotografías, gráficas, cuadros, mapas o muestras materiales.

- **Documental**

Se obtiene por medio de análisis de documentos y se encuentra en cartas, contratos, registros, actas, minutas, facturas, recibos y toda clase de comunicación producto del trabajo. Por lo general, este tipo de información corresponde a aspectos administrativos y contables, aunque también se emplea para verificar que la forma de operar de las organizaciones auditadas coincida con sus registros internos.

- **Testimonial**

Se consigue de toda persona que realiza declaraciones durante la aplicación de la auditoría. Se refiere a los datos derivados de las entrevistas y los cuestionarios realizados en la organización auditada.

- **Analítica**

Comprende cálculos, comparaciones, razonamientos y desagregación de la información por áreas, apartados o componentes. Concierne a la información que más se utiliza en las auditorías administrativas, ya que este tipo de evidencia permite al auditor llegar a conclusiones a través del análisis y comparación de datos. Asimismo, por la metodología que se sigue para obtenerla, la evidencia puede ser directa o indirecta, en lo que se conoce como pruebas de auditoría.

La evidencia directa vincula en forma lógica una proposición o hallazgo con un dato con el cual pueda compararse. Una evidencia indirecta que favorece una proposición o hallazgo es la que coincide con ella sin ser comparable.

Para que la evidencia sea útil y válida, debe ser suficiente, competente, relevante y pertinente.

- ✓ **Evidencia suficiente:** La necesaria para sustentar las observaciones, conclusiones y recomendaciones del auditor. Es indispensable que sea confiable, fehaciente, coherente y susceptible de ser confirmada.
- ✓ **Evidencia competente:** Es consistente, convincente, confiable y ha sido validada, capaz de persuadir sobre su validez para apoyar las conclusiones y recomendaciones del auditor.
- ✓ **Evidencia relevante:** Se trata de la que es importante, coherente y aporta elementos de juicio para demostrar o refutar un hecho en forma lógica y patente.
- ✓ **Evidencia pertinente:** Relaciona la materia revisada y el periodo de la auditoría. Asimismo, surge cuando existe congruencia entre las observaciones, conclusiones y recomendaciones de la auditoría.

2.2.7 Marco Normativo

"NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS, GRUPO 400 (Actividades de Control), SUBGRUPO 410 (Tecnología de la Información)." (Contraloria General del Estado, 2009, págs. 73-83) *(VER ANEXO 3)*

CAPÍTULO III: MARCO METODOLÓGICO

3.1 IDEA A DEFENDER

3.1.1 Idea General

La Auditoria Informática de las Tecnologías de Información y Comunicación en la Dirección Provincial del ambiente de Pastaza, período 2013, comprobará que no se está dando cumplimiento a las normas y leyes establecidas.

3.1.2 Ideas Específicas

- ✓ Los procesos administrativos de uso y manejo de las TIC existentes son erróneos.
- ✓ La vulnerabilidad de la información de la entidad se encuentra ampliamente comprometida.
- ✓ La emisión del informe ayuda a corregir errores detectados.

3.2 VARIABLES

3.2.1 Variable Independiente

- ✓ Auditoría Informática

3.2.2 Variable Dependiente

Cumplimiento de normas y leyes (Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos, Emitidas por la Contraloría General del Estado, Grupo 400 Actividades de Control; sub grupo 410 Tecnología de la Información.

3.3 TIPO DE INVESTIGACIÓN

- **Descriptiva**

Se utiliza este tipo de Investigación ya que nos ayuda a obtener una interpretación correcta del nivel de cumplimiento de Normas y Leyes y por ende nos ayuda a resolver la hipótesis planteada.

- **De Campo**

Se aplica esta investigación por lo que se levantara la información necesaria directamente en las instalaciones de la Dirección del MAE-Pastaza así como también directamente de los empleados y funcionarios de esta dependencia, aplicando las diferentes herramientas a utilizar en esta investigación.

- **Documental**

Para obtener un mejor resultado de la investigación se utilizará libros, tesis, páginas web para obtener información, que nos ayude a resolver la hipótesis planteada.

3.4 POBLACIÓN Y MUESTRA

Con el fin de obtener un resultado preciso y objetivo el examen de Auditoría Informática se aplicó a todos y cada uno de los funcionarios y trabajadores que conforman la dirección provincial del MAE-PASTAZA.

3.5 MÉTODOS, TÉCNICAS E INSTRUMENTOS

3.5.1 Métodos

Método Deductivo

Este método nos permite analizar casos y hechos generales hasta llegar a casos y hechos particulares de nuestra investigación, así con el propósito de señalar las verdaderas particularidades existentes en la unidad informática de la Dirección Provincial del MAE-Pastaza.

Método Inductivo

Este método nos permite analizar casos y hechos particulares y se eleva a casos y hechos generales. De esta forma tenemos una mejor perspectiva de los hechos y estado del área sujeta a investigación.

3.5.2 Técnicas

- **Observación directa**

Se efectuara visitas a las instalaciones de la Dirección del MAE-PASTAZA, con el objeto de obtener una apreciación directa de las actividades y registrar los datos observados, analizarlos e interpretarlos.

- **Encuestas**

Se aplicará a todo el personal involucrado con la unidad Informática del MAE-PASTAZA.

- **Entrevistas**

Durante el desarrollo de la investigación, se realizará entrevistas al personal de la Dirección Provincial del MAE-PASTAZA involucrados en la administración, manejo, uso y custodia de los recursos tecnológicos.

3.5.3 Instrumentos

- **Cuestionarios**

Se utilizará formulario pre-elaborado e impreso, destinado a obtener respuestas sobre el problema en estudio.

- **Cédula de Entrevista**

Se diseña un documento para plasmar y medir opiniones sobre eventos o hechos específicos de la investigación.

CAPÍTULO IV: MARCO PROPOSITIVO

4.1 "AUDITORÍA INFORMÁTICA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN EN LA DIRECCIÓN PROVINCIAL DEL AMBIENTE DE PASTAZA, PERÍODO 2013".

CLIENTE:

- **Dirección Provincial del Ambiente de Pastaza**

ÁREA:

- **Unidad Informática**

PERÍODO:

- **Año 2013**

Figura 1: Propuesta de Auditoría

Fuente: MAE-PASTAZA
Elaborado por: César Mauricio Cajamarca Lema

4.1.1 Orden de trabajo

ORDEN DE TRABAJO N° 0001-MC

Riobamba, 01 de Diciembre del 2014

Estimado
César Mauricio Cajamarca Lema
EGRESADO DE LA EICA
Presente

De mi consideración:

En cumplimiento del Proyecto de Tesis aprobado por el Consejo Directivo de la Facultad de Administración de Empresas, Escuela de Ingeniería en Contabilidad y Auditoría CPA, sírvase proceder a efectuar la *Auditoría Informática de las Tecnologías de Información y Comunicación en la Dirección Provincial del Ambiente de Pastaza,* cuyo alcance cubrirá el período comprendido desde el 01 de Enero al 31 de Diciembre del 2013.

Se faculta al Sr, César Mauricio Cajamarca Lema que actué en calidad de Investigador-Auditor y el suscrito como Supervisor.

Terminado el Trabajo de Auditoría, se servirá presentar el respectivo informe.

Atentamente,

Lic. Iván Patricio Arias González
DIRECTOR TRABAJO DE TITULACIÓN

Ing. Hítalo Bolívar Veloz Segovia
MIEMBRO DE TRIBUNAL

Pastaza, 01 de Diciembre del 2014

PARA: DR. PABLO LÓPEZ
DIRECTOR PROVINCIAL DEL MAE-PASTAZA

DE: SR. MAURICIO CAJAMARCA
INVESTIGADOR-AUDITOR

ASUNTO: INICIO DE LA AUDITORÍA INFORMÁTICA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.

En cumplimiento a la Orden de Trabajo N°0001-MC emitida por el Lic. Iván Arias y el Ing. Hítalo Veloz, catedráticos de la Escuela Superior Politécnica de Chimborazo, Director y Miembro del tribunal de Trabajo de Titulación respectivamente, pongo en consideración que en esta fecha se da inicio a la práctica de Auditoría Informática de las Tecnologías de Información y Comunicación a la unidad informática/tecnológica de la Dirección Provincial del MAE-PASTAZA, cuyo alcance comprende el período entre el 01 de Enero al 31 de Diciembre del 2013.

Particular que pongo en su conocimiento y por su intermedio al personal a su cargo.

A la vez me permito solicitar su colaboración para facilitarme la información que considere necesaria para el éxito de la presente auditoría.

Atentamente,

César Mauricio Cajamarca Lema
EGRESADO DE LA EICA

4.1.2 Plan de la auditoría

PLAN DE AUDITORÍA

ENTIDAD:	DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA
TIPO DE TRABAJO:	Auditoría Informática de las tecnologías de Información y comunicación.
RUBRO O ÁREA:	Unidad Informática/Tecnológica
PERÍODO:	Del 01 de Enero al 31 de Diciembre del 2013
RESPONSABLE:	César Mauricio Cajamarca Lema

1. ANTECEDENTES

En la Dirección Provincial del MAE-PASTAZA no se ha aplicado una Auditoría Informática de las tecnologías de la información y comunicación.

La auditoría Informática en la Dirección Provincial del MAE-PASTAZA, se efectuará de conformidad con la Orden de Trabajo N°. 0001-MC emitida por el Lic. Iván Arias y el Ing. Hítalo Veloz, en calidad de Director y Miembro del tribunal de Tesis respectivamente.

2. MOTIVO DE LA AUDITORÍA

La realización de la Auditoría Informática de las Tecnologías de la Información y Comunicación a la Dirección Provincial del MAE-PASTAZA, se llevará a efecto conforme la Orden de Trabajo N°. 0001-MC, emitida por el Lic. Iván Arias y el Ing. Hítalo Veloz, en calidad de Director y Miembro del tribunal de Trabajo de Titulación respectivamente; y, conforme a un trabajo práctico previo a la obtención del Título de Ingeniería en Contabilidad y Auditoría; por esta razón se efectuará la Auditoria cumpliendo con los parámetros establecidos, normas reglamentarias, procedimientos necesarios de acuerdo a las circunstancias del estudio, posteriormente medir el nivel de cumplimiento de las Normas de Control Interno Emitidas Por la Contraloría General del Estado y emitir un Informe con conclusiones y Recomendaciones que puedan contribuir con la consecución de metas y objetivos planteados por la institución.

3. OBJETIVOS DE LA AUDITORÍA

El Objetivo de realizar una Auditoria Informática a la Dirección Provincial del MAE-PASTAZA, es evaluar la seguridad lógica, seguridad física, el uso y administración de las Tics, en función a las Normas de Control Interno Emitidas por la Contraloría General del Estado determinando así el grado de cumplimiento de dichas normas.

4. ALCANCE DE LA AUDITORÍA

La auditoría Informática de las Tecnologías de la Información y Comunicación que se realizara a la Dirección Provincial del MAE-PASTAZA, comprende el período del 01 de Enero al 31 de Diciembre del 2013.

5. LOCALIZACIÓN DE LA DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

Se encuentra localizada en la Región Amazónica del Ecuador, en la Provincia de Pastaza, Cantón Pastaza, Parroquia Puyo.

6. ESTRUCTURA ORGÁNICA DE LA DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

Para cumplir una eficaz rectoría y gestión ambiental la dirección Provincial del MAE-PASTAZA se estructura de la siguiente forma:

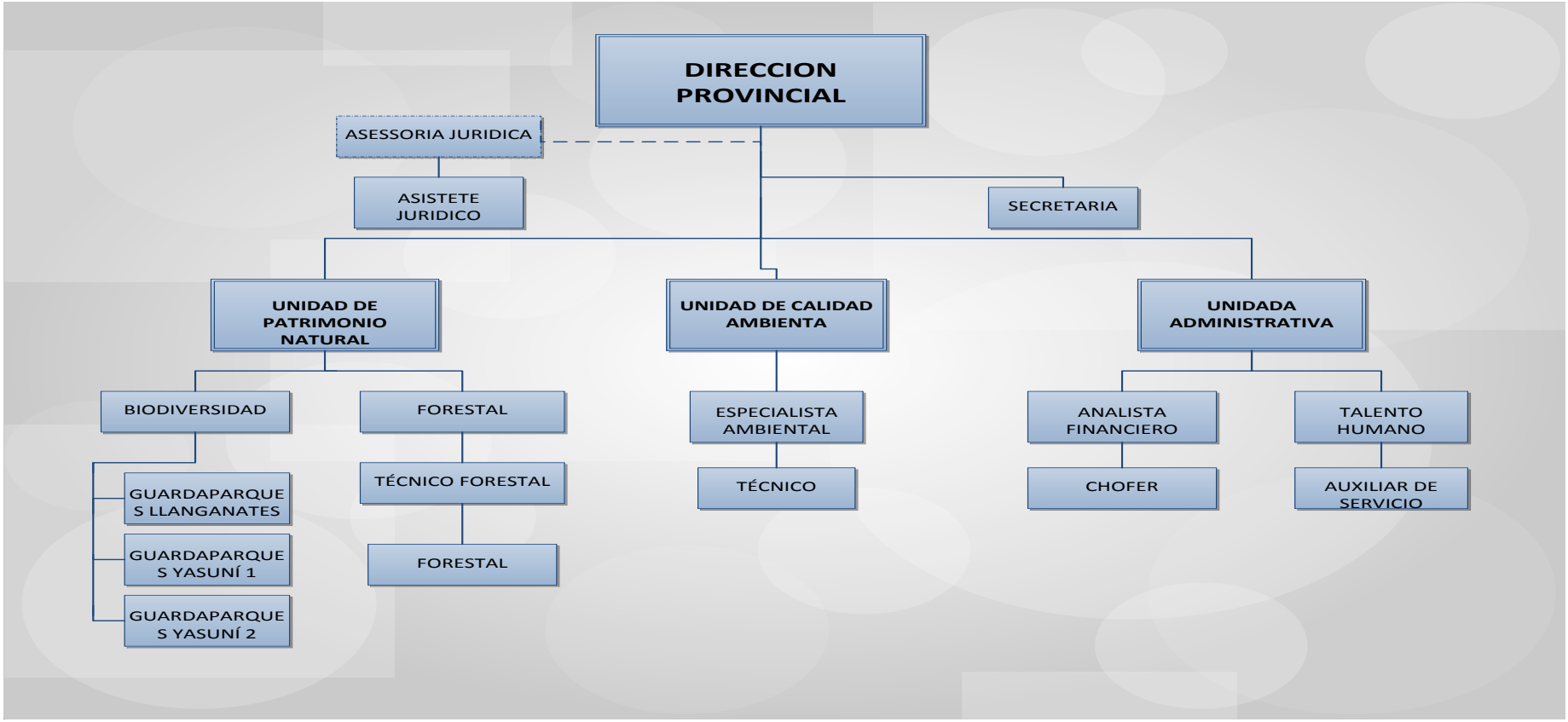


Figura 2: Organigrama Estructural dirección provincial del MAE-PASTAZA
Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

7. MISIÓN, VISIÓN, OBJETIVOS Y VALORES (Ministerio del Ambiente)

Misión

Ejercer de forma eficaz y eficiente la rectoría de la gestión ambiental, garantizando una relación armónica entre los ejes económicos, social, y ambiental que asegure el manejo sostenible de los recursos naturales estratégicos.

Visión

Lograr que el Ecuador use sustentablemente sus recursos naturales estratégicos para alcanzar el Buen vivir.

Objetivos

- ✓ Incorporar los costos y beneficios ambientales y sociales en los indicadores económicos, que permitan priorizar actividades productivas de menos impacto y establecer mecanismos de incentivo adecuados.
- ✓ Generar información sobre la oferta de recursos naturales estratégicos renovables por ecosistema para su manejo integra
- ✓ Reducir la vulnerabilidad ambiental, social y económica frente al cambio climático, concienciar a la población sobre causas y efectos de este fenómeno antropogénico y fomentar la reducción de las emisiones de gases de efecto invernadero en los sectores productivos y sociales.
- ✓ Reducir el consumo de recursos (electricidad, agua y papel) y de producción de desechos.
- ✓ Manejar la conflictividad socio ambiental a través de la incorporación de los enfoques de la participación ciudadana, e interculturalidad y/o género en los proyectos de gestión ambiental.
- ✓ Definir y determinar información e investigación válidas y pertinentes para mejorar la gobernanza ambiental en los ámbitos de la normativa, la dinámica internacional y la participación ciudadana.
- ✓ Fortalecer la institucionalidad del Ministerio del Ambiente.

Valores

- **Legalidad:** los funcionarios y funcionarias, servidores y servidoras públicos del Ministerio del Ambiente trabajarán en forma responsable y conforme los lineamientos, normas, políticas reglamentos y disposiciones legales, sin favorecer ni perjudicar a nadie de manera injusta.
- **Rendición de cuentas:** todos los funcionarios y funcionarias, servidores y servidoras públicos del Ministerio del Ambiente deben informar y documentar sus actividades y decisiones, aceptando e incluso facilitando la revisión, análisis y evaluación de sus acciones y resultados.
- **Calidad:** todos los funcionarios y funcionarias, servidores y servidoras públicos del Ministerio del Ambiente deben preocuparse por exceder los requerimientos y necesidades de sus clientes externos e internos.
- **Compromiso**: lograr el compromiso de todos los actores involucrados, así como la apropiación de responsabilidades en las acciones determinadas en el Plan Estratégico.
- **Relevancia:** destacar que la nueva visión del ministerio del ambiente evocada en el manejo sustentable de los ecosistemas, tiene un importante impacto en garantizar los derechos de la naturaleza y promover un ambiente sano y sustentable.
- **Participación:** promover la participación de los funcionarios del MAE, integrando al proceso a todos los involucrados (funcionarios del Ministerio de Planta Central y de Coordinaciones generales Zonales y Direcciones Provinciales).
- **Académico:** tener presente para la implementación de los equipos funcionales los aportes académicos con base epistemológica sólida y reconocida.

8. BASE LEGAL Y RELACIONAMIENTO INSTITUCIONAL

El Ministerio del Ambiente se encuentra bajo la supervisión del Ministerio Coordinador de Patrimonio, además de reportar los avances de su gestión a corto y mediano plazo a la Secretaría General de la Administración Pública y a la Secretaría Nacional de Planificación y Desarrollo, respectivamente. En lo referente a su relacionamiento con las demás Carteras de Estado establece lazos de cooperación con SENAGUA, Ministerio de Turismo, Secretaría Nacional de Pueblos, Movimientos Sociales y Participación Ciudadana, Ministerio de Educación, Secretaría Nacional de Gestión de

Riesgos y Ministerio de Industrias y Productividad con los cuales puede emprender programas, proyectos y acciones conjuntas de acuerdo a sus competencias.

Por otra parte, y cumpliendo con su rol de AUTORIDAD AMBIENTAL NACIONAL, tiene a su haber la regulación y el control (licenciamiento ambiental) de los proyectos que lleven a cabo los ministerios de Recursos No Renovables, de Transporte y Obras Públicas, Ministerio de Electrificación y Energía Renovable, Ministerio de Agricultura, Ganadería, Acuicultura y Pesca y Ministerio de Desarrollo Urbano y Vivienda, así como de aquellos proyectos desarrollados por los Gobiernos Autónomos Descentralizados y particulares que de acuerdo a la ley lo requiriesen. Finalmente, depende del Ministerio de Economía y Finanzas en cuanto a la asignación de recursos, y de las disposiciones del Ministerio de Relaciones Internacionales, Comercio Exterior y Competitividad para asumir una posición país frente a los diferentes temas de la Agenda Ambiental Internacional.

El ministerio del ambiente al ser una institución pública es regido por varias instancias normativas que rigen el Ecuador, por lo que para la presente investigación nos enfocamos puntualmente a las Normas de control Interno emitidas por la Contraloría General del Estado, grupo de las 400 y sub grupo 410 que son las que enmarcan normativamente al recurso tecnológica de las instituciones públicas. *(VER ANEXO 3)*

9. FACULTADES, PRODUCTOS Y SERVICIOS DE LA DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

- **Facultades:** gestión, control técnico.
- **Principales productos y servicios:** Biodiversidad conservada a través del Sistema Nacional de Áreas Protegidas, Vida Silvestre conservada a través del control y manejo sustentable in situ y ex situ, Licencias de aprovechamiento forestal, Incentivos a la Conservación del Recurso Forestal, Recursos Forestales Manejados Sustentablemente, Fichas Ambientales, Licencias Ambientales (trámites), Control y Seguimiento del Cumplimiento de las Normas de Calidad Ambiental, Implementación de Programa Nacional de Adaptación al Cambio Climático, Implementación del Programa Nacional de Mitigación al Cambio Climático.

10. RECURSO UTILIZADO

- **Recurso Humano**

✓ Director y Miembro de tribunal de trabajo de titulación, quienes actúan como guías y supervisores de auditoría.

✓ El autor (investigador/auditor) egresado de la Escuela de Contabilidad y Auditoría de la ESPOCH.

- **Recursos Materiales**

✓ Resma de Papel Bond

✓ Esferos gráficos (azul, rojo)

✓ Agenda de notas

✓ Carpetas/Archivadores

- **Recursos Financieros**

✓ El investigador/auditor asume el financiamiento total de la investigación.

- **Recurso Tecnológico**

✓ Computador

✓ Internet

11. TIEMPO ESTIMADO

La presente auditoría informática se efectuara en un período de 90 días a partir del 01 de Diciembre del 2014, en donde se realizó:

- Estudio preliminar.
- Revisión de la legislación, objetivos, políticas y normas.
- Examen de áreas críticas.
- Comunicación de resultados.

César Mauricio Cajamarca Lema
ELABORADO POR

Lic. Iván Arias e Ing. Hítalo Veloz
REVISADO POR

4.2 FASES DE AUDITORIA

ÍNDICES DE AUDITORÍA INFORMÁTICA

Tabla 3: índices de auditoría informática

ÍNDICES Y ABREVIATURAS		
ÍNDICE	**ETAPA**	**DESCRIPCIÓN**
E1	I	Planeación de Auditoría Informática.
E2	II	Ejecución de Auditoría Informática.
E3	III	Dictamen o resultados de Auditoría Informática.
P.A		Programa de Auditoría
C.C.I.S.L		Cuestionario de control interno seguridad lógica
C.C.I.S.F		Cuestionario de control interno seguridad física
C.C.I.T.I		Cuestionario de control interno Tecnologías de la información
C.C.I.G.I		Cuestionario de control interno Gestión Informática
C.C.I.ADM.		Cuestionario de control interno Administración (usuarios)
M.P		Matriz de ponderación
M.R		Matriz de riesgo
E.F		Entrevista funcionario
E.P		Entrevista al personal
H.H		Hoja de hallazgo
DNR SL		Determinación del nivel de riesgo seguridad lógica
DNR SF		Determinación del nivel de riesgo seguridad física
DNR TI		Determinación del nivel de riesgo tecnologías de la información
DNR GI		Determinación del nivel de riesgo Gestión Informática
DNR ADM		Determinación del nivel de riesgo seguridad Administración.
DNR TI		Determinación de nivel de riesgo de Tecnologías de Información.
M.P ADM		Matriz de ponderación Administración

Fuente: Varios Autores
Realizado por: César Mauricio Cajamarca Lema

MARCAS DE AUDITORÍA INFORMÁTICA

Tabla 4: Marcas de auditoría informática

MARCA	SIGNIFICADO/INTERPRETACIÓN
✓	Verificado una vez
√	Verificado dos veces
✓✓	Dato Correcto
X	Dato con error
N/A	No aplica
≠	Diferencias Detectadas
A	Documento analizado
θ	Observación
Δ	Hallazgo

Fuente: Varios Autores
Realizado por: César Mauricio Cajamarca Lema

SIGLAS DE AUDITORÍA INFORMÁTICA

Tabla 5: Siglas de auditoría informática

SIGLAS	EQUIPO DE TRABAJO	CARGO
A.G.I.P.	Arias Gonzales Iván Patricio	Supervisor de Auditoría
C.L.C.M.	Cajamarca Lema César Mauricio	Auditor Senior

Fuente: Varios Autores
Realizado por: César Mauricio Cajamarca Lema

4.2.1 PRIMERA ETAPA: Planeación de Auditoría Informática.

AUDITORÍA INFORMÁTICA PROGRAMA DE AUDITORÍA Del 1 de Enero al 31 de Diciembre del 2013	E1 (1/6) P.A 1/1

ENTIDAD AUDITADA: Dirección Provincial del MAE-PASTAZA
FASE I: Planeación

No.	DESCRIPCIÓN	REF. P.T	REALIZADO POR	FECHA
	OBJETIVOS			
	Conocer de primera fuente la operatividad en general del Área Informática de la institución, con el fin de dar inicio a la Auditoria Informática.			
	PROCEDIMIENTOS			
1	Realizar una carta al Director Provincial del MAE-PASTAZA, con el fin de dar a conocer el inicio de la auditoria y solicitar la información y facilidades necesarias.	E1 2/6	C.L.C.M.	01/12/2014
2	Solicitud y análisis del organigrama estructural de la Institución.	E1 3/6 a 4/6	C.L.C.M.	05/12/2014
3	Solicitud y análisis del manual de funciones del área Informática.	E1 5/6	C.L.C.M.	06/12/2014
4	Solicitud y análisis de políticas y procedimientos del área Informática.	E1 6/6	C.L.C.M.	06/12/2014

Elaborado por:	C.L.C.M	**Fecha:**	01/12/2014
Revisado por:	A.G.I.P	**Fecha:**	02/12/2014

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE I: PLANEACIÓN

CARTA AL DIRECTOR

Pastaza, 01 de Diciembre del 2014

DR.
Pablo López
DIRECTOR PROVINCIAL DEL MAE-PASTAZA
Presente

De mi consideración

La presente Auditoria se enfocara al Área Informática de manera que el beneficio sea para las dos partes involucradas.

La Auditoria Informática se realizara con el fin de determinar el grado de cumplimiento de las normas de control interno emitidas por la Contraloría General del Estado grupo 410 en lo que respecta a tecnologías de información y comunicación, relacionados con la seguridad lógica, seguridad física, aprovechamiento y utilización de las Tics y gestión de la informática, para lo cual se aplicara encuestas, entrevistas, revisión de documentos y análisis de los mismos que de sustento a la evidencia encontrada.

Así mismo se solicita de la manera más comedida la suficiente colaboración y facilidades por parte de los funcionarios y trabajadores que se desempeñan en esta área.

Por la oportuna y ágil acogida a la presente extiendo mis agradecimientos.

Atentamente,

Mauricio Cajamarca
AUDITOR

Elaborado por:	C.L.C.M	**Fecha:**	01/12/2014
Revisado por:	A.G.I.P	**Fecha:**	02/12/2014

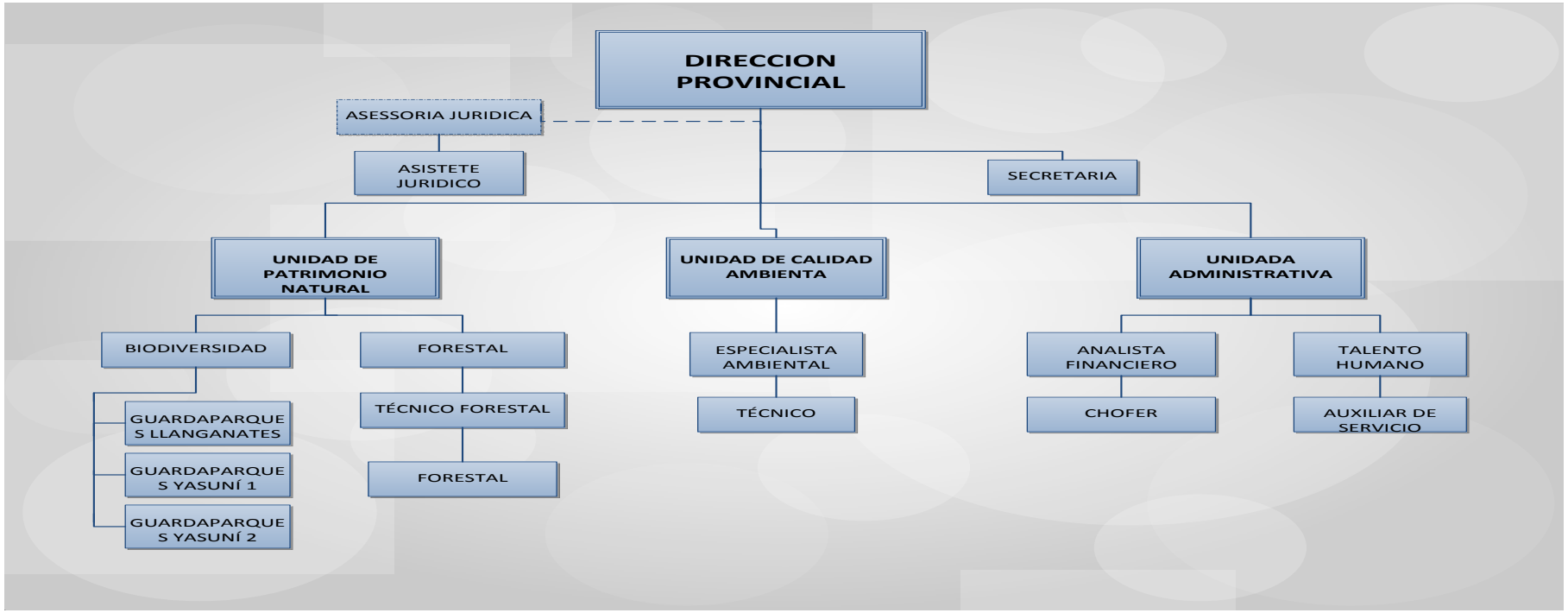
E1 3/6

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE I: PLANEACIÓN

ORGANIGRAMA DE LA DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA ~~AΔ~~



Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

E1 4/6

~~A~~ ΔEl Organigrama orgánico funcional de la Dirección Provincial del MAE-PASTAZA no se establece o identifica una unidad para este fin por lo que no cumple con la norma 410-01 de Organización Informática, donde menciona, *"La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección*".

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE I: PLANEACIÓN

MANUAL DE FUNCIONES DEL ÁREA INFORMÁTICA DE LA DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA~~A~~

ANALISTA DE TECNOLOGÍAS PROVINCIAL

MISIÓN:

Ejecutar actividades de desarrollo y mantenimiento de software de forma sistemática y productiva, asegurando su calidad, fiabilidad y facilidad de uso de los sistemas informáticos, tecnologías de la información y comunicación.

FUNCIONES:

A) Controla mecanismos en los sistemas automatizados, accesos, bases de datos, redes y comunicaciones.
B) Administra y mantiene a los usuarios de los sistemas de información.
C) Brinda soporte de mantenimiento de los sistemas informáticos que apoyan a diferentes unidades o direcciones del ministerio.
D) Elabora y ejecuta programas de capacitación de los sistemas informáticos y tecnológicos a los servidores de la institución para que pueda ejecutarlos y operarlos en forma segura y adecuada.
E) Mantiene actualizada y en custodia la documentación técnica y del usuario de los sistemas de información en operación.
F) Administra redes de comunicación, correo electrónico, internet, base de datos y otros servicios instalados.
G) Realiza cableado y equipos que conforman la infraestructura básica de la red informática del MAE.
H) Verifica el mantenimiento y actualización del sitio Web institucional. ~~A~~ *(VER ANEXO 2)*

Elaborado por:	C.L.C.M	**Fecha:**	06/12/2014
Revisado por:	A.G.I.P	**Fecha:**	07/12/2014

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE I: PLANEACIÓN

POLÍTICAS Y PROCEDIMIENTOS DEL ÁREA INFORMÁTICA DE LA DIRECCIÓN PROVINCIAL DEL MAE-PASTAZAΔ

ΔLas políticas y procedimientos de área Informática de la Dirección Provincial del MAE-PASTAZA no existen, a decir del funcionario encargado de dicha unidad esta documentación reposa en Dirección General en la ciudad de Quito las mismas que no son entregadas y socializadas a cada dirección provincial.

Elaborado por:	C.L.C.M	**Fecha:**	06/12/2014
Revisado por:	A.G.I.P	**Fecha:**	07/12/2014

4.2.2 SEGUNDA ETAPA: Ejecución de Auditoría Informática.

AUDITORÍA INFORMÁTICA
PROGRAMA DE AUDITORÍA
Del 1 de Enero al 31 de Diciembre del 2013

E2 1/47
P.A 1/2

ENTIDAD AUDITADA: Dirección Provincial del MAE-PASTAZA
FASE II: Ejecución de Auditoria Informática

N°	DESCRIPCIÓN	REF. PT.	ELABORADO POR:	FECHA	OBSERVACIÓN
OBJETIVO					
	Determinar y analizar el cumplimiento de normas referentes a la seguridad lógica, seguridad física, buen uso y administración del recurso tecnológico.				
PROCEDIMIENTOS					
1	Aplicar encuesta al director del y encargado de las TIC,S del MAE-PASTAZA, enfocado al área Informática.	**E2 3/47 a 4/47**	**C.L.C.M**	**05/12/2014**	
2	Aplicar encuestas a los trabajadores que dan uso directa e indirectamente los recursos tecnológicos, referente a:				
	• Seguridad Lógica	**E2 5/47 a 7/47**	**C.L.C.M**	**05/12/2014**	
	• Seguridad Física.	**E2 8/47 a 10/47**	**C.L.C.M**	**05/12/2014**	
	• Tecnologías de Información y comunicación.	**E2 11/47 a 13/47**	**C.L.C.M**	**05/12/2014**	
	• Gestión Informática	**E2 14/47 a 16/47**	**C.L.C.M**	**05/12/2014**	
	• Administrativo (Usuarios)	**E2 17/47 a 26/47**	**C.L.C.M**	**05/12/2014**	
3	Solicitar y verificar los procesos y políticas de asignación y cambio de claves de acceso.	**E2 27/47**	**C.L.C.M**	**07/12/2014**	

					E2 2/47 P.A 1/2
N°	**DESCRIPCIÓN**	**REF. PT.**	**ELABORADO POR:**	**FECHA**	**OBSERVACIÓN**
4	Realizar verificación física sobre medidas de seguridad para las tic´s.	**E2 28/47**	**C.L.C.M**	**07/12/2014**	
5	Solicitar la Planificación del mantenimiento de Instalaciones y Equipos.	**E2 29/47**	**C.L.C.M**	**07/12/2014**	
6	Solicite las Políticas de documentación y eliminación de archivo.	**E2 30/47**	**C.L.C.M**	**07/12/2014**	
7	Solicitar el cronograma de actividades, metas y objetivos del área de Informática.	**E2 31/47**	**C.L.C.M**	**07/12/2014**	
8	Solicitar los Planes de contingencia.	**E2 32/47**	**C.L.C.M**	**07/12/2014**	
9	Solicitar planes de capacitaciones.	**E2 33/47**	**C.L.C.M**	**07/12/2014**	
10	Solicitar inventario de Infraestructura tecnológica.	**E2 34/47**	**C.L.C.M**	**07/12/2014**	
11	Determinación el nivel de Riesgo y nivel de confianza del área Informática.	**E2 35/47 a 36/47**	**C.L.C.M**	**09/05/2015**	
12	Realizar matriz de riesgos	**E2 37/47 a 39/47**	**C.L.C.M**	**09/05/2015**	
13	Determinar Hallazgos	**E2 40/47 A 47/47**	**C.L.C.M**	**09/05/2015**	

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

E2 3/47
E.F 1/2

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

Entrevista aplicada al Director Provincial del MAE-PASTAZA.

OBJETIVO: Obtener información general del área Informática.

1. **¿Con que objetivo se crea el área informática en el MAE-PASTAZA?**
   El área informática existe en planta central.

2. **¿Existe misión, visión, objetivos y políticas establecidas para el área informática?**
   Si existe.

3. **De existir misión, visión, objetivos y políticas, ¿Cuáles son?**
   Lo tienen en planta central.

4. **De no existir misión, visión, objetivos y políticas, ¿Cuáles son las razones?**
   Si existe.

5. **¿Quiénes son los funcionarios y trabajadores que colaboran en esta área?**

   El funcionario en cargado de la unidad tecnológica es el ing. Jorge Pullas.

6. **¿Cuáles son las responsabilidades y funciones de los colaboradores?**

   Revisar el sistema informático

   NOTA: *Si las respuestas no presentan los documentos pertinentes, se tomara la misma como negativas.*

E2 4/47
E.F 2/2

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

Entrevista aplicada al responsable del área informática del MAE-PASTAZA.

OBJETIVO: Obtener información general del área Informática.

1. **¿Con que objetivo se crea el área informática en el MAE-PASTAZA?**
   Dar soporte de primer nivel para la dirección Provincial, descentralizarlo.

2. **¿Existe misión, visión, objetivos y políticas establecidas para el área informática?**
   Sí, pero es la misma del ministerio del ambiente.

3. **De existir misión, visión, objetivos y políticas, ¿Cuáles son?**
   Aparte de la Misión y Visión del MAE existen políticas como seguridad de la información, acuerdos de seguridad informática, entre otros.
4. **De no existir misión, visión, objetivos y políticas, ¿Cuáles son las razones?**
   No contesta.
5. **¿Quiénes son los funcionarios y trabajadores que colaboran en esta área?**
   Técnico informático.

6. **¿Cuáles son las responsabilidades y funciones de los colaboradores?**

   Velar por el funcionamiento, uso, seguridad y control de las tecnologías de información del ministerio.

   NOTA: *Si las respuestas no presentan los documentos pertinentes, se tomara la misma como negativas.*

CUESTIONARIO DE CONTROL INTERNO					E2 5/47 C.C.I. SL ½
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Seguridad Lógica				
Objetivo:	Verificar la existencia y aplicación de las medidas para contrarrestar las amenazas que pueda afectar la integridad de los datos e información de la entidad.				

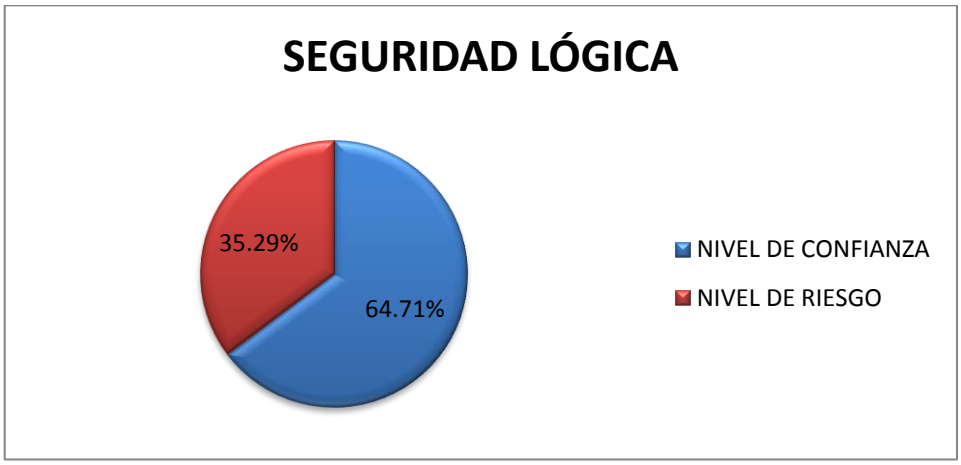
N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿El sistema operativo de los ordenadores cumple con las características necesarias para el desarrollo de las actividades?	X			
2	¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?		X		
3	¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal?	X			
4	¿Existen procedimientos de notificación y gestión de incidencias?		X		
5	¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos e información?		X		
6	¿Existe personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?	X			
7	¿Se realizan controles periódicos para verificar el cumplimiento de procesos y normas?		X		
8	¿Existen medidas y/o procedimiento a adoptar cuando se agregue o suprime aplicaciones y/o software que modifique parcial o total los ordenadores?	X			
9	¿Se restringe el acceso a personal no autorizado a acceder a las instalaciones donde se encuentren ubicados los sistemas informáticas que guardan información de la institución?	X			
		Elaborado por:		C.L.C.M	**Fecha:** 05/12/2014
		Revisado por:		A.G.I.P	**Fecha:** 06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 6/47 C.C.I. SL 2/2
10	¿Se restringe el acceso a ordenadores donde se guarda el soporte de datos e información?	X			
11	¿Existe un período máximo caducidad de las contraseñas de acceso?	X			
12	¿Existe una clasificación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos?	X			
13	¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas, y las mismas están debidamente documentadas?		X		
14	¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?	X			
15	¿En el sistema están habilitadas para todas las cuentas de usuario las opciones que permiten establecer: • Un número máximo de intentos de conexión. • Un período máximo de vigencia para la contraseña.	X			
16	¿Existen procedimientos de asignación y distribución de contraseñas?	X			
17	¿Se realizan auditorías a los archivos de seguridad?		X		
TOTAL		**16**	**11**		

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

- **DETERMINACIÓN DE NIVEL DE RIESGO Y CONFIANZA DE SEGURIDAD LÓGICA.**

Preguntas positivas	11	64.71%
Preguntas negativas	6	35.29%
TOTAL	17	100%



Gráfica 1: Nivel de confianza de seguridad lógica

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

Tabla 6: nivel de confianza seguridad lógica

NIVEL DE CONFIANZA SEGURIDAD LÓGICA			
NC=	64.71	%	**MEDIO**
NIVEL DE RIESGO SEGURIDAD LÓGICA			
NR =	35.29	%	**BAJO**

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

ANÁLISIS: Con lo que respecta la seguridad lógica se obtiene un nivel de confianza del 64,71 % de nivel de confianza y un 35,29% de nivel de riesgo.

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 8/47 C.C.I. SF 1/2
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Seguridad Física				
Objetivo:	Revisar las políticas y Normas sobre seguridad Física, seguridad de personal, datos, hardware, software e instalaciones.				

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Se han adoptado medidas de seguridad para salvaguardar los sistemas de información?	X			
2	¿Existe una persona responsable de la seguridad?	X			
3	¿Existe personal de vigilancia en la institución?	X			
4	¿Se investiga a los vigilantes cuando son contratados?	X			
5	¿Existe vigilancia en las instalaciones las 24 horas?	X			
6	¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?	X			
7	¿Se registra el acceso al área informática de personas ajenas a la dirección?		X		
8	¿Se vigilan la moral y comportamiento del personal con el fin de mantener una buena imagen y evitar un posible fraude?		X		
9	¿Existe un sistema de ventilación adecuado para los equipos e instalaciones?		X		
10	¿Existen extintores de fuego en las instalaciones?	X			
11	¿Se ha capacita y entrenado al personal en el manejo de los extintores?	X			

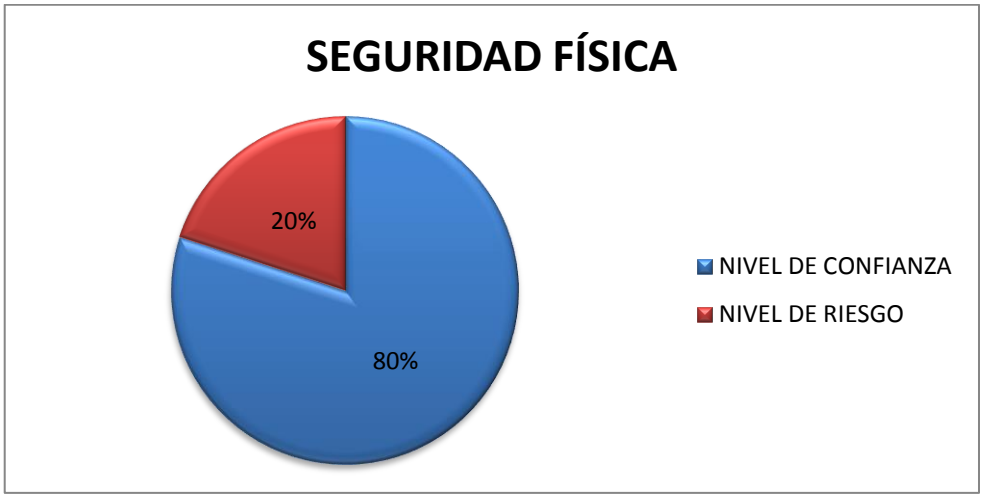
		Elaborado por:	**C.L.C.M**	**Fecha:**	05/12/2014
		Revisado por:	**A.G.I.P**	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 9/47 C.C.I. SF 2/2
12	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstrucciones?	X			
13	¿El personal sabe qué hacer en caso de que ocurra una emergencia ocasionado por fuego?	X			
14	¿El personal ajeno a operación sabe qué hacer en el caso de un incendio?	X			
15	¿Existe salida de emergencia?		X		
16	¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas?	X			
17	¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior de las instalaciones a fin evitar daños a los equipos?	X			
18	¿Se limpia con frecuencia el polvo acumulado en lugares de difícil acceso para evitar daños a los equipos?	X			
19	¿Existen procedimientos para la realización de las copias de seguridad?		X		
20	¿Hay procedimientos que aseguran la realización de copias de todos aquellos datos que han experimentado algún cambio en su contenido?	X			
21	¿Existen controles sobre el acceso físico a las copias de seguridad?	X			
22	¿Existe un inventario de los soportes existentes?	X			
23	¿Dicho inventario incluye las copias de seguridad?	X			
24	¿Existen procedimientos de etiquetado e identificación del contenido de los soportes?	X			
25	¿Se Verifica que todos los soportes cuenten con claves de acceso?	X			
TOTAL		**20**	**5**		

Elaborado por:	**C.L.C.M**	**Fecha:**	05/12/2014
Revisado por:	**A.G.I.P**	**Fecha:**	06/12/2014

- **DETERMINACIÓN DE NIVEL DE RIESGO Y CONFIANZA DE SEGURIDAD FÍSICA.**

Preguntas positivas	20	80%
Preguntas negativas	5	20%
TOTAL	25	100%



Gráfica 2: nivel de confianza seguridad física

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

Tabla 7: **Nivel de confianza seguridad física**

NIVEL DE CONFIANZA SEGURIDAD FÍSICA			
NC=	80	%	**MEDIO**
NIVEL DE RIESGO SEGURIDAD FÍSICA			
NR =	20	%	**MEDIO**

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

ANÁLISIS: Realizado la ponderación pertinente se determina en la seguridad física un nivel de confianza del 80% y un nivel de riego del 20%.

CUESTIONARIO DE CONTROL INTERNO					E2 11/47 C.C.I. TI 1/2
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Tecnologías de Información				
Objetivo:	Conocer aspectos relacionados a la utilización y aprovechamiento de los recursos informáticos a fin de determinar si los equipos disponibles son actualizados y si existen políticas establecidas para su utilización.				

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existe un plan logístico para el mantenimiento preventivo/correctivo del software?	X			
2	¿Existe un plan logístico para el mantenimiento preventivo/correctivo para el hardware e instalaciones?	X			
3	¿Los planes de mantenimiento se cumplen a cabalidad?		X		
4	¿Existen procedimientos para solucionar daños o fallas existentes en los equipos?	X			
5	¿Existe tiempos establecidos para la solución de problemas presentados en los equipos?	X			
6	¿Se mantienen planes de limpieza adecuados a fin de evitar la acumulación de polvo en los equipos?	X			
7	¿Los equipos existentes son suficientes para la operatividad de la institución?	X			
8	¿Existe suficiente mobiliario para la operatividad y desenvolvimiento de los sistemas informáticos?		X		
9	¿Existen políticas que norme el trabajo definidas del personal que labora en esta área?	X			
10	¿Existe políticas, manuales y procesos de utilización y uso de los equipos informáticos?		X		

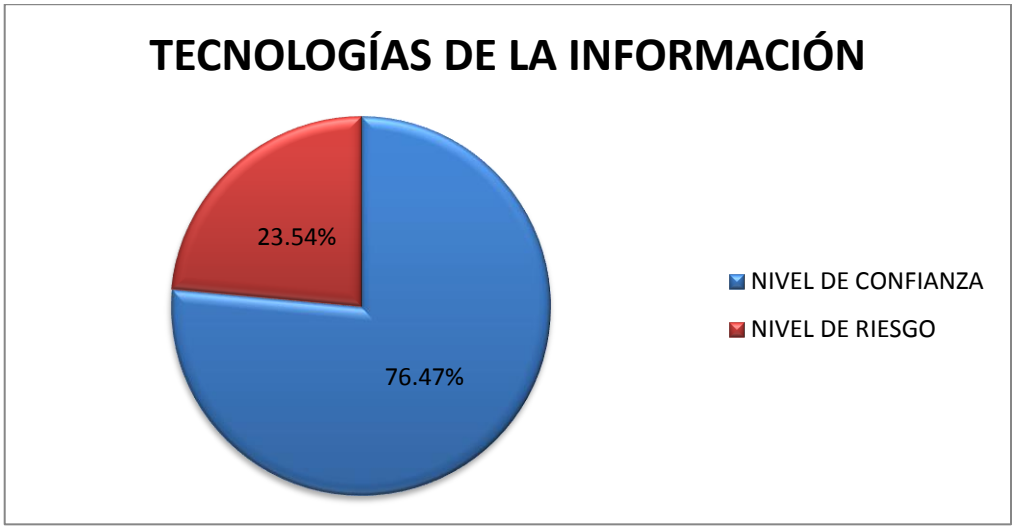
		Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
		Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 12/47 C.C.I. TI 2/2
11	¿El software (programas) disponibles en los ordenadores de la institución contribuyan a las actividades diarias de la misma?	X			
12	¿Existe software ofimática (programas y herramientas informáticas de oficina) actualizado que estén disponibles para los empleados y funcionarios de la institución?	X			
13	¿Existe software utilitario que sea de apoyo y que estén disponibles para los empleados y funcionarios?	X			
14	¿La información transmitida por internet es controlada?	X			
15	¿Se elabora normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitios WEB en base a las disposiciones legales?		X		
16	¿Se considera el desarrollo de aplicaciones WEB y/o móviles que automaticen los procesos o tramites orientados al uso de instituciones y ciudadanos en general?	X			
17	¿El servicio de Internet satisface las necesidades de la institución?	X			
TOTAL		**13**	**4**		

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

- **DETERMINACIÓN DE NIVEL DE RIESGO Y CONFIANZA DE TECNOLOGÍAS DE INFORMACIÓN.**

Preguntas positivas	13	76.47%
Preguntas negativas	4	23.53%
TOTAL	17	100%



Gráfica 3: Nivel de confianza tecnologías de Información

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

Tabla 8: **nivel de confianza tecnologías de información**

NIVEL DE CONFIANZA TECNOLOGÍAS DE INFORMACIÓN			
NC=	76,47	%	ALTO
NIVEL DE RIESGO TECNOLOGÍAS DE INFORMACIÓN			
NR =	23,53	%	**BAJO**

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

ANÁLISIS: Luego de realizar la ponderación de las tecnologías de Información se obtiene un nivel de confianza del 76,47% y un nivel de riego del 23,53%.

CUESTIONARIO DE CONTROL INTERNO					E2 14/47 C.C.I GI 1/2
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Gestión Informática				
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.				

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Se desarrolla regularmente planes a corto, medio y largo plazo que apoyen el logro de la misión, visión y metas de la institución?	X			
2	¿Dispone la institución de un plan Estratégico de Tecnología de Información?	X			
3	¿La planificación del área informática, está en función del plan estratégico de toda la institución?	X			
4	¿Las tareas y actividades plasmadas en el plan tiene la correspondiente y adecuada asignación de recursos?	X			
5	¿Existe un comité de informática?		X		
6	¿Existen estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y actualizados?	X			
7	¿Las descripciones de los puestos de trabajo reflejan las actividades realizadas en la práctica?	X			
8	¿Existen controles que tienden a asegurar que el cambio de puesto de trabajo y la finalización de los contratos laborales no afectan a los controles internos y a la seguridad informática?	X			
9	¿Existe un presupuesto económico para la adquisición de nuevos bienes? ¿Y hay un proceso para elaborarlo?	X			

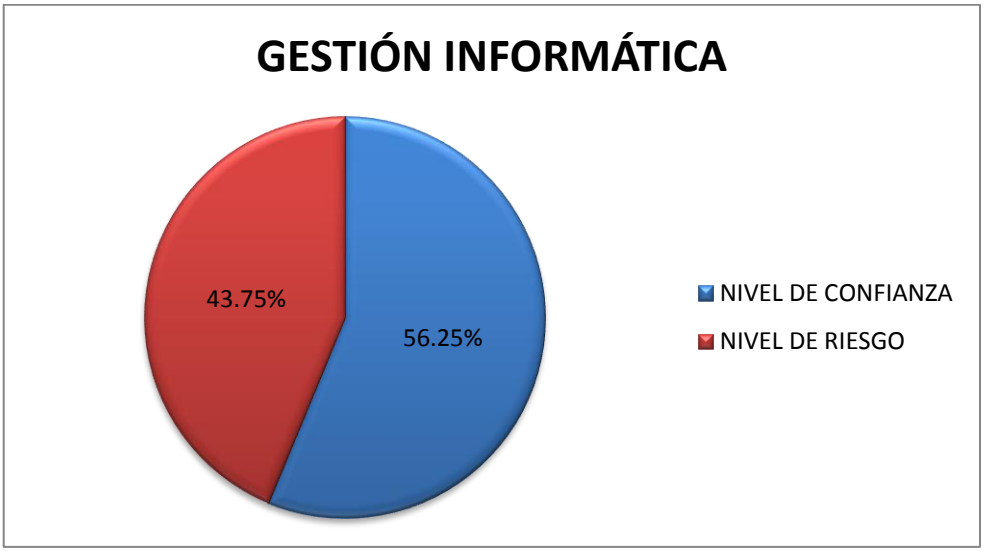
		Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
		Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 15/47 C.C.I. GI 2/2
10	¿Existen procedimientos para la adquisición de bienes y servicios?		X		
11	¿Existe un plan operativo anual?		X		
12	¿Existe un cronograma de cumplimiento de metas?		X		
13	¿Se comprueban los resultados con datos reales?		X		
14	¿Existe un organigrama con la estructura de organización del área?		X		
15	¿El presupuesto está en concordancia con los objetivos a cumplir?	X			
16	¿Existen procedimientos para vigilar y determinar permanentemente la normativa aplicable?		X		
TOTAL		**9**	**7**		

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

- **DETERMINACIÓN DE NIVEL DE RIESGO Y CONFIANZA DE LA GESTIÓN INFORMÁTICA.**

Preguntas positivas	9	56.25%
Preguntas negativas	7	43.75%
TOTAL	16	100%



Gráfica 4: Nivel de confianza gestión informática

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

Tabla 9: **Nivel de confianza de gestión informática**

NIVEL DE CONFIANZA DE GESTIÓN INFORMÁTICA			
NC=	56.25	%	ALTO
NIVEL DE RIESGO DE GESTIÓN INFORMÁTICA			
NR =	43.75	%	**BAJO**

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

ANÁLISIS: En la gestión informática se obtiene como resultado un nivel de confianza del 56,25% y un nivel de riego del 43,75%.

CUESTIONARIO DE CONTROL INTERNO					E2 17/47 C.C.I ADM 1/8
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Administración/usuarios (UNIDAD FINANCIERA)				
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.				
N°	**PREGUNTAS**	**RESPUESTAS**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?		X		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?		X		
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?		X		
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?		X		
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	X			
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?		X		
TOTAL		**6**	**6**		

Preguntas positivas	6	50%
Preguntas negativas	6	50%
TOTAL	12	100%

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 18/47 C.C.I ADM 2/8
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Administración/usuarios (SECRETARIA)				
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.				
N°	**PREGUNTAS**	**RESPUESTAS**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?	X			
2	¿Se aprueban solicitudes de nuevas aplicaciones?		X		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?		X		
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?		X		
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	X			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?		X		
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL		**8**	**4**		

Preguntas positivas	8	66.67%
Preguntas negativas	4	33.33%
TOTAL	12	100%

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 19/47 C.C.I ADM 3/8
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Administración/usuarios (ASISTENTE JURÍDICO)				
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.				
N°	**PREGUNTAS**	**RESPUESTAS**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?	X			
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?		X		
4	¿Existen procedimientos adecuados para mantener la documentación al día?		X		
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	X			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?		X		
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL		**8**	**4**		

Preguntas positivas	8	66.67%
Preguntas negativas	4	33.33%
TOTAL	12	100%

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 20/47 C.C.I ADM 4/8
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Administración/usuarios (ESPECIALISTA AMBIENTAL)				
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.				
N°	**PREGUNTAS**	**RESPUESTAS**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?	X			
2	¿Se aprueban solicitudes de nuevas aplicaciones?	X			
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	X			
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	X			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?		X		
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL		**11**	**1**		

Preguntas positivas	11	91.67%
Preguntas negativas	1	8.33%
TOTAL	12	100%

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 21/47 C.C.I ADM 5/8
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Administración/usuarios (ANALISTA DE TALENTO HUMANO)				
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.				

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?		X		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?		X		
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?		X		
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?		X		
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL		**7**	**5**		

Preguntas positivas	7	58.33%
Preguntas negativas	5	41.67%
TOTAL	12	100%

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 22/47 C.C.I ADM 6/8
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Administración/usuarios (UNIDAD DE CALIDAD AMBIENTAL)				
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.				
N°	**PREGUNTAS**	**RESPUESTAS**			**OBSERVACIONES**
		SI	**NO**	**N/A**	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?		X		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	X			
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?		X		
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	X			
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL		**9**	**3**		

Preguntas positivas	9	75%
Preguntas negativas	3	25%
TOTAL	12	100%

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 23/47 C.C.I ADM 7/8
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Administración/usuarios (ESPECIALISTA CALIDAD AMBIENTAL)				
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.				

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?	X			
2	¿Se aprueban solicitudes de nuevas aplicaciones?	X			
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	X			
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	X			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	X			
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL		**12**	**0**		

Preguntas positivas	12	100%
Preguntas negativas	0	0.00%
TOTAL	12	100%

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

CUESTIONARIO DE CONTROL INTERNO					E2 24/47 C.C.I ADM 8/8
Entidad:	Dirección Provincial del MAE-PASTAZA				
Área evaluada:	Informática/Tecnológica				
Tipo de Auditoría:	Auditoría Informática				
Componente:	Administración/usuarios (COORDINADOR PATRIMONIO CULTURAL)				
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.				

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?		X		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	X			
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	X			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	X			
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL		**10**	**2**		

Preguntas positivas	10	83.33%
Preguntas negativas	2	16.67%
TOTAL	12	100%

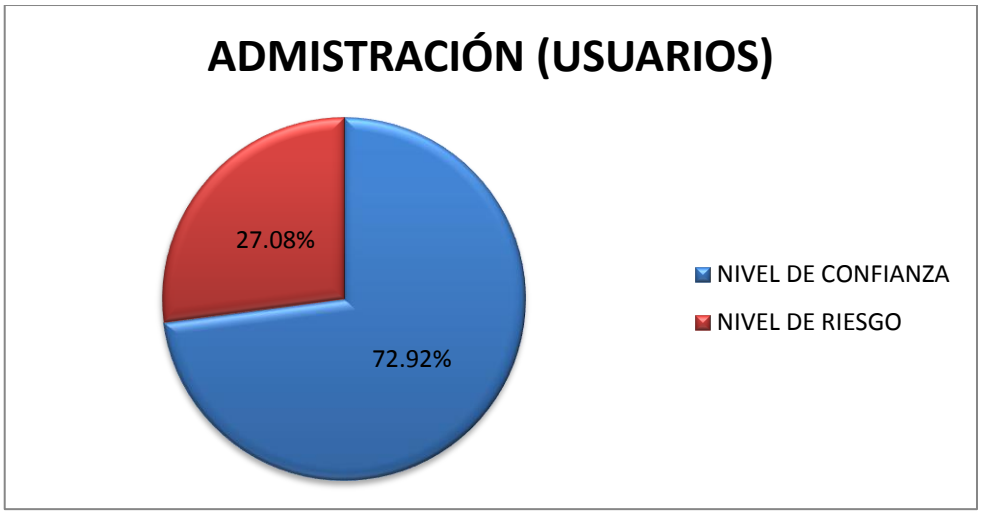
Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

MATRIZ DE PONDERACIÓN (ADMINISTRACIÒN)			F2 25/47 M.P ADM 1/1
N°	**PREGUNTAS**	**RESPUESTAS POSITIVAS**	**RESPUESTAS NEGATIVAS**
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?	3	5
2	¿Se aprueban solicitudes de nuevas aplicaciones?	3	5
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	3	5
4	¿Existen procedimientos adecuados para mantener la documentación al día?	7	1
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	6	2
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	8	0
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	5	3
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	8	0
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	4	4
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	8	0
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	8	0
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	7	1
	TOTAL	**70**	**26**

Elaborado por:	C.L.C.M	**Fecha:**	05/12/2014
Revisado por:	A.G.I.P	**Fecha:**	06/12/2014

- **DETERMINACIÓN DE NIVEL DE RIESGO Y CONFIANZA DE ADMINISTRACIÓN (USUARIOS).**

Preguntas positivas	70	72,92%
Preguntas negativas	26	27,08%
TOTAL	96	100%



Gráfica 5: Nivel de confianza administración (usuarios)

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

Tabla 10: Nivel de confianza de administración (usuarios)

NIVEL DE CONFIANZA DE ADMINISTRACIÓN (USUARIOS)			
NC=	72,92	%	MEDIO
NIVEL DE RIESGO DE ADMINISTRACIÓN (USUARIOS)			
NR =	27,08	%	**BAJO**

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

ANÁLISIS: Una vez realizada las encuestas a ocho funcionarios de los diferentes departamentos del MAE-PASTAZA se determina un nivel de confianza del 72,92% y un nivel de riesgo del 27,08%.

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

VERIFICACIÓN DE PROCESOS Y POLÍTICAS DE ASIGNACIÓN Y CAMBIO DE CLAVES DE ACCESO.Δ

Esta verificación no pudo ser aplicada, ya que, a decir del funcionario encargado de las tecnologías de Información estos documentos reposan en la dependencia general del Ministerio del Ambiente en la ciudad de Quito, los mismos no son estregados y socializados en esta dependencia provincial.

ΔPor lo que se concluye que dichos procedimientos y políticas no existen.

Elaborado por:	C.L.C.M	**Fecha:**	07/12/2014
Revisado por:	A.G.I.P	**Fecha:**	08/12/2014

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

Tabla 11: **Verificación física sobre medidas de seguridad para las tic´s.**

Tipologías	Complemento	Cumple		Observaciones
		si	No	
Seguridad	Existe una persona que custodie los bienes de la unidad informática. (guardia)	X		
	Existe un circuito cerrado de cámaras de vigilancia.		X	No funcionan
	El espacio físico donde se encuentra la unidad Informática está en buenas condiciones.		X	Espacio inadecuado
	Existen adecuadas salidas de emergencia.	X		
	Existen extintores contra incendios.		X	
	Existen alarmas contra incendios y/o robos.	X		
Accesos	Existe un adecuado control de acceso para funcionarios y trabajadores de la unidad.	X		Control diario de firmas
	Existen restricciones a usuarios externos.		X	
	Las puestas y ventanales cuentas con las debidas seguridades del caso.	X		
Sistema Eléctrico	El conjunto de cables de la institución se encuentra oculto y debidamente identificado.	X		
	Existen reguladores de voltaje que salvaguarden los equipos de la institución.	X		
	Los puntos de iluminación son adecuados	X		
Otros	El sistema de ventilación es adecuado		X	
	Los equipos tecnológicos e instalaciones en general cuentan con una póliza de seguros.		X	No se entrega contrato
	Existen las herramientas e instalaciones para dar mantenimiento a los equipos.		X	

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

SOLICITAR LA PLANIFICACIÓN DEL MANTENIMIENTO DE INSTALACIONES Y EQUIPOS. Δ

Este procedimiento no pudo ser aplicada, ya que, a decir del funcionario encargado de las tecnologías de Información no existe un planificación realizada para los debidos mantenimientos de equipos e instalaciones, además menciono que cuando un equipo requiere de mantenimiento esto se debe notificar a la dependencia general de la ciudad de Quito para que se tome las respectivas accione del caso.

ΔPor lo que se concluye que dicha planificación no existen.

Elaborado por:	C.L.C.M	**Fecha:**	07/12/2014
Revisado por:	A.G.I.P	**Fecha:**	08/12/2014

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

SOLICITE LAS POLÍTICAS DE DOCUMENTACIÓN Y ELIMINACIÓN DE ARCHIVO. Δ

Este procedimiento no pudo ser aplicada, por la no existencia de documentación alguna. El manejo de la documentación y eliminación de los archivos está a juicio del funcionario que maneja su documentación y equipo respectivo.

ΔPor lo que se concluye que dicha planificación no existen.

Elaborado por:	C.L.C.M	**Fecha:**	07/12/2014
Revisado por:	A.G.I.P	**Fecha:**	08/12/2014

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

SOLICITAR EL CRONOGRAMA DE ACTIVIDADES, METAS Y OBJETIVOS DEL ÁREA DE INFORMÁTICA. Δ

Este procedimiento no pudo ser aplicada, ya que, en la respectiva entrevista el funcionario encargado menciona que la unidad informática en si no cuenta con metas y objetivos planteados, menciono que trabajan con las metas y objetivos planteadas con la institución en general.

ΔPor lo que se concluye que dicho cronograma no existen.

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

SOLICITAR LOS PLANES DE CONTINGENCIA. Δ

Este procedimiento no pudo ser aplicado, ya que dichos planes de contingencia no son realizados por la unidad informática.

ΔPor lo que se concluye que los planes de contingencia no existen.

Elaborado por:	C.L.C.M	**Fecha:**	07/12/2014
Revisado por:	A.G.I.P	**Fecha:**	08/12/2014

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

SOLICITAR PLANES DE CAPACITACIONES. Δ

Este procedimiento no pudo ser aplicado, ya que, hasta el momento no se han ejecutado ninguna capacitación para el manejo adecuado de los equipos tecnológicos de la institución.

ΔPor lo que se concluye que dichos reportes no existen.

Elaborado por:	C.L.C.M	**Fecha:**	07/12/2014
Revisado por:	A.G.I.P	**Fecha:**	08/12/2014

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

SOLICITAR INVENTARIO DE INFRAESTRUCTURA TECNOLÓGICA. Δ

Este procedimiento no pudo ser aplicado, ya que, a decir del funcionario de las tecnologías de la información estos documentos reposan en la dependencia general en la ciudad de Quito.

ΔPor lo que se concluye que dichos inventarios no existen.

Elaborado por:	C.L.C.M	**Fecha:**	07/12/2014
Revisado por:	A.G.I.P	**Fecha:**	08/12/2014

AUDITORÍA INFORMÁTICA

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

DETERMINACIÓN EL NIVEL DE RIESGO Y NIVEL DE CONFIANZA DEL ÁREA INFORMÁTICA.

Tabla 12: Ponderación de las encuestas aplicadas

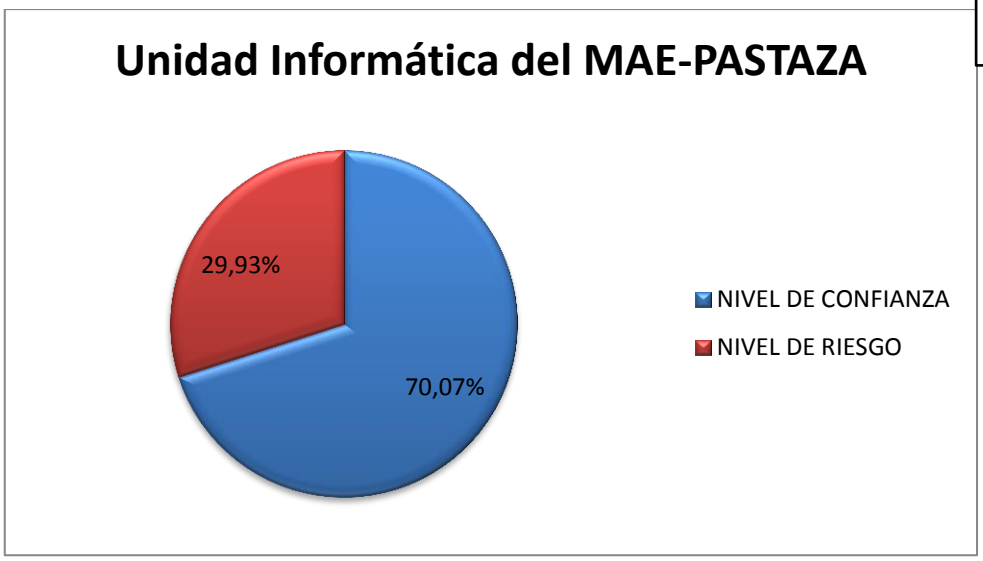
PONDERACIÓN DE LAS ENCUESTAS APLICADAS		
COMPONENTES	**NIVEL DE CONFIANZA %**	**NIVEL DE RIESGO %**
SEGURIDAD LÓGICA	64,71	35,29
SEGURIDAD FÍSICA	80	20
TECNOLOGÍAS DE LA INFORMACIÓN	76,47	23,53
GESTIÓN INFORMÁTICA	56,25	43,75
ADMINISTRACIÓN (USUARIOS)	72,92	27,08
TOTAL	**350,35**	149,65
PROMEDIO	**70,07**	**29,93**

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

Tabla 13: niveles de confianza y riesgo

RIESGO	CALIFICACIÓN	CONFIANZA
BAJO	**15% al 50%**	BAJO
MEDIO	**51% al 75%**	MEDIO
ALTA	**76% al 95%**	ALTA

Fuente: Varios autores
Realizado por: César Mauricio Cajamarca Lema



Gráfica 6: Nivel de confianza de la unidad informática del MAE-PASTAZA

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

Tabla 14: **nivel de confianza de la unidad informática del MAE-PASTAZA**

NIVEL DE CONFIANZA DE LA UNIDAD INFORMÁTICA DEL MAE-PASTAZA			
NC=	70.07	%	MEDIO
NIVEL DE RIESGO DE LA UNIDAD INFORMÁTICA DEL MAE-PASTAZA			
NR =	29,93	%	**BAJO**

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

ANÁLISIS: Una vez aplicadas las encuestas a los componentes de Seguridad Lógica, Seguridad Física, Gestión Informática, Tecnologías de Información y al área administrativa (usuarios) y realizado las ponderaciones respectivas se determina un nivel de confianza para el área informática del 70,07% y un nivel de riego del 29,93%.

E2 37/47
M.R 1/3

Tabla 15: MATRIZ DE RIESGOS

REF PT	TÍTULO HALLAZGO	CAUSA	EFECTO	ACCIONES RECOMENDADAS	NORMA RELACIONADA
E1 3/6 a 4/6	Ausencia de identificación de la unidad informática en el organigrama estructural del MAE-PASTAZA.	La Dirección Provincial no establece e identifica una unidad informática dentro del organigrama institucional	No se encuentra el apoyo necesario en cuanto a las tic´s para mejorar la operatividad de esta unidad.	La dirección debe gestionar e identificar dentro del organigrama institucional en un nivel de apoyo a esta a la unidad informática.	410-01 Organización Informática.
E1 6/6	Inexistencia de políticas y procedimientos que regulen las actividades relacionadas con las tecnologías de información.	La dirección Provincial y el encargado de las TIC´S no promueven y establecen políticas y procedimientos que normen las actividades de esta unidad.	Los datos e información no son salvaguardados adecuadamente, así como también la operatividad en general de la unidad está comprometida.	La Dirección y el funcionario encargado de esta unidad deben definir, documentar y difundir políticas y procedimientos que den los lineamientos necesarios a las actividades propias de esta unidad.	410-04 Políticas y Procedimientos.
E2 29/47; E2 34/47	Falta de planes de mantenimiento tanto preventivo y/o correctivo, así como también un inventario de control de bienes informáticos existentes.	El funcionario encargado de la unidad informática no define planes de mantenimientos preventivos y/o correctivos, así como también no mantiene un control de los bienes informáticos debidamente inventariados	Perdidas de información, tiempo y recursos al deteriorarse los equipos, datos equívocos e imprecisos de las existencias y control de los bienes.	El funcionario de la unidad informática deberá establecer planes de mantenimiento y levantar un inventario exacto de los bienes existentes en la unidad Informática.	410-09 Mantenimiento y control de la infraestructura tecnológica.

E2 38/47
M.R 2/3

E2 28/47; **E2 30/47**	Falta de mecanismos de seguridad necesario que protejan y salvaguarden la información que se procesa mediante los sistemas informáticos de la institución.	El funcionario encargado de la unidad Informática no establece los mecanismos necesarios para salvaguardar los datos e información de la institución.	Perdida de los datos e información que se procesa en los sistemas informáticas de la institución.	El funcionario de la unidad informática debe establecer los mecanismos necesarios para salvaguardar la información de la institución.	410-10 seguridades de Tecnologías de Información.
E2 32/47	Falta de definir e implementar planes de contingencia que describan las acciones a tomar en caso de emergencia.	El funcionario encargado de la unidad informática no define e implementa planes de contingencia que describan las acciones a tomar en caso de emergencia.	Inadecuada toma de decisiones en caso de emergencias o problemas presentados en equipos, instalaciones o personal relacionado, que desemboca en pérdidas de información y operatividad de la unidad.	El funcionario de la unidad informática deberá implementar planes de contingencia donde se describan las acciones a tomar en caso de emergencias suscitadas.	410-11 Plan de contingencias.
E2 31/47	Falta de definir y ejecutar mecanismos, cronogramas donde se mida el grado de contribución al cumplimiento de metas y objetivos institucionales.	El funcionario encargado de la unidad informática no define ni ejecuta los mecanismos necesarios para medir el grado de contribución del cumplimiento de metas y objetivos institucionales.	La unidad informática no aportando adecuadamente a la consecución de metas y objetivos planteados por la institución.	El funcionario encargado de la unidad informática deberá definir y ejecutar los mecanismos necesarios para medir el grado de contribución a la consecución de metas y objetivos institucionales.	410-13 Monitoreo y evaluación de los procesos y servicios.

E2 39/47
M.R 3/3

E2 11/47 a 13/47	Falta de establecer normas, procedimiento e instructivos de instalación, configuración, y utilización de los servicios de internet, correos electrónicos y sitios WEB de la entidad.	El funcionario encargado de la unidad informática no establece normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, correos electrónicos, y sitos WEB de la entidad.	Mal uso de los sitios de internet que puedes afectar y dañar parcial o totalmente a los equipos informáticos, así como también fuga y/o pérdida de información propia de la institución.	El funcionario encargado de la unida informática deberá establecer normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, correos electrónicos y sitios WEB de la institución.	410-14 Sitios web, servicios de internet e intranet.
E2 33/47	Inexistencia de planes de capacitación tanto a usuarios internos como externos de la unidad informática.	El director Provincial como el encargado de la unidad informática no proporcionan un plan de capacitación que involucre a todos los usuarios de las tic´s.	Mal manejo y uso de los equipos tecnológicos que pueden comprometer la integridad de la información y de la misma infraestructura tecnológica.	El director provincial conjuntamente con el encargado de la unidad informática deberá proporcionar un plan de capacitación para todos los actores y usuarios de las tecnologías de información de la institución.	410-15 Capacitación Informática.

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

HOJA DE HALLAZGO

TÍTULO 1: FALTA DE IDENTIFICACIÓN DE LA UNIDAD INFORMÁTICA.

CONDICIÓN: No se identifica en el Organigrama Estructural a la unidad de Tecnologías de Información.

CRITERIO: La Dirección Provincial del MAE-PASTAZA debe gestionar e identificar en un nivel de apoyo dentro de su estructura organizacional a la unidad de Tecnologías de Información, conforme establece la Norma de Control Interno 410-01, que concierne a "*Organización Informática*".

CAUSA: La Dirección Provincial del MAE-PASTAZA no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO: No se establece e identifica una unidad Informática dentro de su estructura organizacional por lo que se dificulta la transparencia, estandarización y control de las Tecnologías de Información del MAE-PASTAZA.

Elaborado por:	C.L.C.M	**Fecha:**	09/05/2015
Revisado por:	A.G.I.P	**Fecha:**	10/05/2015

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

HOJA DE HALLAZGO

TÍTULO 2: FALTA DE POLÍTICAS Y PROCEDIMIENTOS.

CONDICIÓN: No se promueven y establecen políticas y procedimientos que normen las actividades de esta unidad.

CRITERIO: La Dirección Provincial y el funcionario encargado de la unidad informática del MAE-PASTAZA deben promover y establecer políticas y procedimientos que regulen las actividades relacionadas con las Tecnologías de Información, conforme establece la Norma de Control Interno 410-04, que concierne a "*Políticas y Procedimientos*".

CAUSA: La Dirección Provincial y el Funcionario encargado de la unidad tecnológica del MAE-PASTAZA no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO: Desorganización, falta de control y lineamientos dentro de todas las actividades que se desarrollan en la unidad de Tecnologías de Información del MAE-PASTAZA, que deja en evidencia la vulnerabilidad de los datos, información e equipos Informáticos que posee la institución.

Elaborado por:	C.L.C.M	**Fecha:**	09/05/2015
Revisado por:	A.G.I.P	**Fecha:**	10/05/2015

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

HOJA DE HALLAZGO

TÍTULO 3: INEXISTENCIA DE PLANES DE MANTENIMIENTO Y CONTROL DE INVENTARIO.

CONDICIÓN: Falta de ejecución y aplicación de Planes de mantenimiento correctivo/preventivo, así como también el control de inventario de los bienes existentes.

CRITERIO: El funcionario encargado de la unidad Informática del MAE-PASTAZA debe definir y ejecutar planes de mantenimiento para toda la infraestructura tecnológica, así como también levantar un inventario de los bienes existentes en la institución, conforme establece la Norma de Control Interno 410-09, que concierne a "*Mantenimiento y control de la infraestructura tecnológica*".

CAUSA: El Funcionario encargado de la unidad tecnológica del MAE-PASTAZA no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO: Daños parciales o totales de la infraestructura tecnológica, pérdida de recursos, datos erróneos e inexactos en la existencia y control de bienes.

Elaborado por:	C.L.C.M	**Fecha:**	09/05/2015
Revisado por:	A.G.I.P	**Fecha:**	10/05/2015

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

HOJA DE HALLAZGO

TÍTULO 4: INEXISTENCIA DE MECANISMOS DE SEGURIDAD.

CONDICIÓN: No se establecen los mecanismos necesarios que salvaguarden los medios Informáticos.

CRITERIO: El funcionario encargado de la unidad Informática del MAE-PASTAZA debe establecer los mecanismos necesarios que ayuden a salvaguardar los medios Informática de la institución, conforme establece la Norma de Control Interno 410-10, que concierne a "*Seguridad de Tecnologías de Información*".

CAUSA: El Funcionario encargado de la unidad tecnológica del MAE-PASTAZA no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO: Pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos existente en la institución.

Elaborado por:	C.L.C.M	**Fecha:**	09/05/2015
Revisado por:	A.G.I.P	**Fecha:**	10/05/2015

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

HOJA DE HALLAZGO

TÍTULO 5: INEXISTENCIA DE PLANES DE CONTINGENCIA.

CONDICIÓN: No define planes de contingencia para que sean ejecutados en casos de emergencias que se susciten en la institución.

CRITERIO: El funcionario encargado de la unidad Informática del MAE-PASTAZA debe establecer y definir planes de contingencias donde se describan los lineamientos a seguir en caso de emergencias suscitadas dentro de la institución, conforme establece la Norma de Control Interno 410-11, que concierne a "*Plan de contingencias*".

CAUSA: El Funcionario encargado de la unidad tecnológica del MAE-PASTAZA no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO: Inadecuada toma de decisiones en caso de emergencias o problemas presentados en equipos, instalaciones o personal relacionado, que desemboca en pérdidas de información y operatividad de la unidad.

Elaborado por:	C.L.C.M	**Fecha:**	09/05/2015
Revisado por:	A.G.I.P	**Fecha:**	10/05/2015

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

HOJA DE HALLAZGO

TÍTULO 6: INEXISTENCIA DE MONITOREO Y EVALUACIÓN DE PROCESOS.

CONDICIÓN: Falta de sistemas de monitoreo y evaluación a los procesos operativos de la unidad Informática.

CRITERIO: El funcionario encargado de la unidad Informática del MAE-PASTAZA debe definir y ejecutar sistemas de monitoreo y evaluación donde se determine el grado de operatividad de la unidad Tecnológica de la institución, conforme establece la Norma de Control Interno 410-13, que concierne a "*Monitoreo y evaluación de los procesos y servicios.*"

CAUSA: El Funcionario encargado de la unidad tecnológica del MAE-PASTAZA no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO: Deficiencias operativas no detectadas en la unidad informática, las mismas que conllevan a un inadecuado aporte a la consecución de metas y objetivos planteados por la institución.

Elaborado por:	C.L.C.M	**Fecha:**	09/05/2015
Revisado por:	A.G.I.P	**Fecha:**	10/05/2015

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

HOJA DE HALLAZGO

TÍTULO 7: FALTA DE CONTROL PARA SITIOS WEB.

CONDICIÓN: Falta de establecer normas, procedimiento e instructivos de instalación, configuración, y utilización de los servicios de internet, correos electrónicos y sitios WEB de la entidad.

CRITERIO: El funcionario encargado de la unidad Informática del MAE-PASTAZA debe establecer normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, correos electrónicos, y sitos WEB de la entidad, conforme establece la Norma de Control Interno 410-14, que concierne a "*Sitios web, servicios de internet e intranet.*"

CAUSA: El Funcionario encargado de la unidad tecnológica del MAE-PASTAZA no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO: Mal uso de los sitios de internet que pueden afectar y dañar parcial o totalmente a los equipos informáticos, así como también fuga y/o pérdida de información propia de la institución.

Elaborado por:	C.L.C.M	**Fecha:**	09/05/2015
Revisado por:	A.G.I.P	**Fecha:**	10/05/2015

ENTIDAD AUDITADA: DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA

FASE II: EJECUCIÓN DE LA AUDITORÍA

HOJA DE HALLAZGOS

TÍTULO 8: FALTA DE CAPACITACIÓN INFORMÁTICA.

CONDICIÓN: Inexistencia de desarrollo y ejecución de planes de capacitación tanto a usuarios internos como externos de la unidad informática.

CRITERIO: La Dirección Provincial y el funcionario encargado de la unidad Informática del MAE-PASTAZA debe desarrollar y ejecutar planes de capacitación donde se integre a todos los usuarios directos e indirectos de las tecnologías de información de la institución, conforme establece la Norma de Control Interno 410-15, que concierne a "*Capacitación Informática.*"

CAUSA: El Funcionario encargado de la unidad tecnológica del MAE-PASTAZA no acata y aplica la ley establecida, puntualmente a la norma referida anteriormente.

EFECTO: Mal manejo y uso de los equipos tecnológicos que pueden comprometer el estado físico de la infraestructura tecnológica y comprometer la integridad de la información.

Elaborado por:	C.L.C.M	**Fecha:**	09/05/2015
Revisado por:	A.G.I.P	**Fecha:**	10/05/2015

4.2.3 TERCERA ETAPA: Dictamen o resultados de Auditoría Informática.

AUDITORÍA INFORMÁTICA **PROGRAMA DE AUDITORÍA** **Del 1 de Enero al 31 de Diciembre del 2013**	**E3** **P.A 1/1**

ENTIDAD AUDITADA: Dirección Provincial del MAE-PASTAZA
FASE III: Dictamen o resultados de Auditoría Informática

No.	DESCRIPCIÓN	REF. P.T	REALIZADO POR	FECHA
	OBJETIVOS			
	Socializar las falencias encontradas en cuanto a la aplicación de normas establecidas para el manejo de las tecnologías de información, a través del informe de auditoría informática con sus respectivas conclusiones y recomendaciones.			
	PROCEDIMIENTOS			
1	Elabore la Carta de Presentación.		C.L.C.M.	11/05/2015
2	Elabore el Informe de Auditoria		C.L.C.M.	12/05/2015
5	Realice el Archivo Correspondiente		C.L.C.M.	12/05/2015

Elaborado por:	C.L.C.M	**Fecha:**	11/05/2015
Revisado por:	A.G.I.P	**Fecha:**	10/05/2015

CARTA DE PRESENTACIÓN

Pastaza, 11 de Junio del 2015

DR.
Pablo López
DIRECTOR PROVINCIAL DEL MAE-PASTAZA
Presente

De mi consideración

He realizado la Auditoría Informática a la DIRECCIÓN PROVINCIAL DEL MAE-PASTAZA por el período comprendido entre Enero a Diciembre 2013.
El análisis se realizó de acuerdo con las Normas de Control Interno emitidas por la Contraloría General del Estado en lo referente a tecnologías de información y comunicación. La evaluación incluye el análisis y estudio de seguridad lógica, seguridad física, utilización y aprovechamiento de tecnologías de información y comunicación Tics y gestión informática.

Debida a la naturaleza de estudio y de los componentes evaluados, los resultados de la auditoria se encuentran en las conclusiones y recomendaciones del presente informe.

Atentamente,

Mauricio Cajamarca
AUDITOR

INFORME CONFIDENCIAL

Pastaza, 12 de Junio del 2015

Emisión del informe de auditoría informática.

1. Al Director Provincial del MAE-PASTAZA, por el período comprendido de Enero a Diciembre 2013, en cuanto a seguridad lógica, seguridad física, aprovechamiento y correcta utilización de las Tecnologías de información y comunicación, y gestión de la informática, la responsabilidad consiste en expresar una opinión sobre los mismos en base a la práctica de la auditoría.

2. El análisis se realizó de acuerdo con las Normas de Control Interno emitidas por la Contraloría General del Estado grupo 410 en lo referente a tecnologías de información y comunicación. Las sintomatologías detectadas a lo largo de la auditoría informática se enfocan a la ausencia e identificación de la unidad informática en el organigrama de la institución, carencia de políticas y procedimientos establecidas que indiquen de manera documentada y debidamente aprobada, el cambio de claves de acceso a los sistemas de información como de correo electrónico y sistema operativo con una periodicidad de tiempo establecida y formalmente comunicada, también políticas y procedimientos de eliminación de archivos que ya no se utilicen, falta de desarrollo y ejecución de planes de mantenimiento, la falta de medidas de seguridad adecuadas para proteger y salvaguardar los bienes que están a disposición del Departamento de Informática, la falta de recursos necesarios para desarrollar una mejor gestión informática cuando se presentan daños o desperfectos en los equipos que reposan en las diferentes unidades de la institución , la ausencia de un control de inventario a la infraestructura tecnológica, la falta de un plan de contingencia en caso de alguna eventualidad que se pueden presentar, la ausencia de capacitaciones tanto a usuarios internos como externos. Se considera que este estudio proporciona una base razonable para expresar la opinión en base a los parámetros establecidos.
3. En mi opinión, los aspectos mencionados en el párrafo anterior son inconsistencias que se deben mejorar a través de la toma de decisiones en base a las recomendaciones emitidas en el presente informe.

Mauricio Cajamarca.
AUDITOR

INFORME DE AUDITORÍA INFORMÁTICA

CAPÍTULO I

Motivo del examen.

La realización de la auditoría Informática a la dirección Provincial del MAE-PASTAZA, se llevó a efecto conforme la Orden de Trabajo N°. 0001-MC, emitida por el Lic. Iván Patricio Arias González (Director de Trabajo de Titilación) y el Ing. Hítalo Bolívar Veloz Segovia (Miembro de tribunal); conforme a una práctica de Trabajo de Titilación previo a la obtención del Título de Ingeniería en Contabilidad y Auditoría; por esta razón se efectuó el examen cumpliendo con los parámetros establecidos, normas reglamentarias(Normas de control interno, 410 tecnologías de la información) , procedimientos necesarios de acuerdo a las circunstancias del estudio, enfocados principalmente a la evaluación de los aspectos de seguridad lógica, seguridad física, correcta utilización de la Tecnologías de Información y Comunicación y la gestión informática, para así posteriormente emitir criterios para contribuir al desarrollo de la unidad tecnológica del MAE-PASTAZA.

Objetivo General

Realizar la Auditoría Informática a la dirección Provincial del MAE-PASTAZA, período 2013, para medir el nivel de cumplimiento de las Normas de Control Interno sobre Tecnologías de la Información.

Objetivos específicos

- Analizar los documentos de soporte que sustentan la propiedad, veracidad y legalidad de las operaciones de gestión informática.
- Evaluar el sistema de control interno existente para el uso, control y resguardo de los Equipos, Sistemas y Paquetes Informáticos.
- Determinar el nivel de cumplimiento de la normativa legal vigente como son las Normas de Control Interno emitidas por la Contraloría General del Estado.

Alcance del Examen

El examen comprendió el análisis a área puntuales como: "Seguridad física, Seguridad Lógica, uso adecuado de Tecnologías de Información y Comunicación y la Gestión Informática", de la dirección Provincial del MAE-PASTAZA, del período comprendido entre 01 de Enero del 2013 al 31 de Diciembre del 2013.

Base Legal

El Ministerio del Ambiente se encuentra bajo la supervisión del Ministerio Coordinador de Patrimonio, además de reportar los avances de su gestión a corto y mediano plazo a la Secretaría General de la Administración Pública y a la Secretaría Nacional de Planificación y Desarrollo, respectivamente. En lo referente a su relacionamiento con las demás Carteras de Estado establece lazos de cooperación con SENAGUA, Ministerio de Turismo, Secretaría Nacional de Pueblos, Movimientos Sociales y Participación Ciudadana, Ministerio de Educación, Secretaría Nacional de Gestión de Riesgos y Ministerio de Industrias y Productividad con los cuales puede emprender programas, proyectos y acciones conjuntas de acuerdo a sus competencias.

Por otra parte, y cumpliendo con su rol de AUTORIDAD AMBIENTAL NACIONAL, tiene a su haber la regulación y el control (licenciamiento ambiental) de los proyectos que lleven a cabo los ministerios de Recursos No Renovables, de Transporte y Obras Públicas, Ministerio de Electrificación y Energía Renovable, Ministerio de Agricultura, Ganadería, Acuicultura y Pesca y Ministerio de Desarrollo Urbano y Vivienda, así como de aquellos proyectos desarrollados por los Gobiernos Autónomos Descentralizados y particulares que de acuerdo a la ley lo requiriesen. Finalmente, depende del Ministerio de Economía y Finanzas en cuanto a la asignación de recursos, y de las disposiciones del Ministerio de Relaciones Internacionales, Comercio Exterior y Competitividad para asumir una posición país frente a los diferentes temas de la Agenda Ambiental Internacional.

El ministerio del ambiente al ser una institución pública es regido por varias instancias normativas que rigen el Ecuador, por lo que para la presente investigación nos enfocamos puntualmente a las Normas de control Interno emitidas por la Contraloría General del Estado, grupo de las 400 y sub grupo 410 que son las que enmarcan normativamente al recurso tecnológica de las instituciones públicas.

Estructura Orgánica

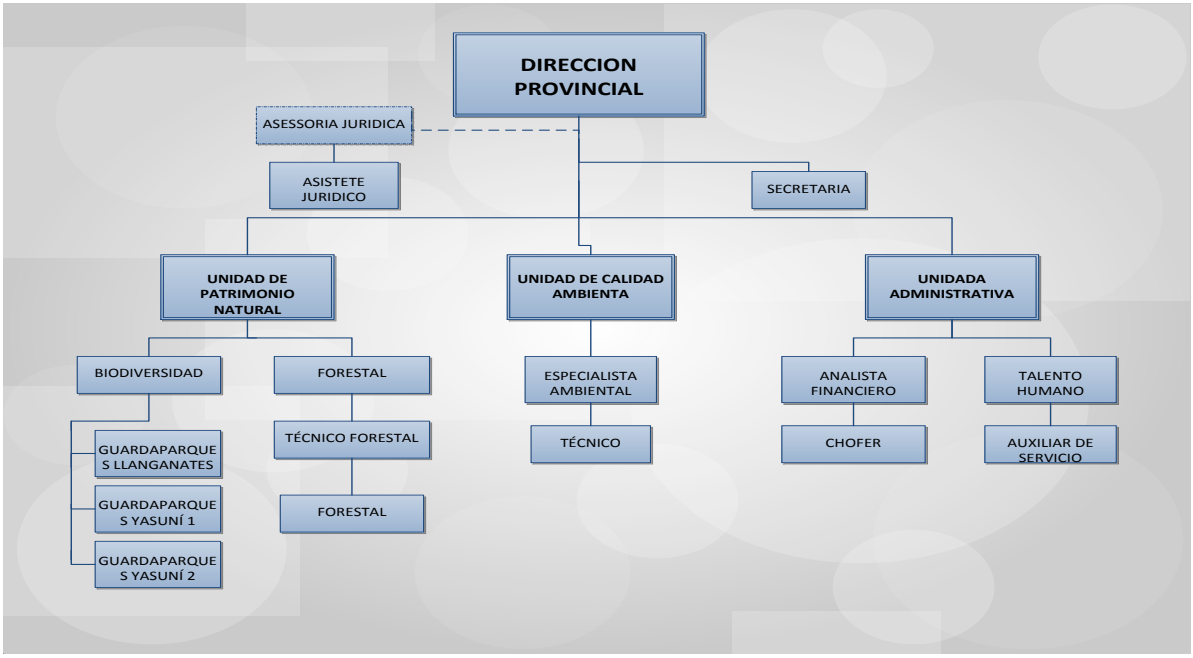


Figura 2: Organigrama Estructural dirección provincial del MAE-PASTAZA

Fuente: MAE- PASTAZA
Realizado por: César Mauricio Cajamarca Lema

Cultura Organizacional.

Misión

Ejercer de forma eficaz y eficiente la rectoría de la gestión ambiental, garantizando una relación armónica entre los ejes económicos, social, y ambiental que asegure el manejo sostenible de los recursos naturales estratégicos.

Visión

Lograr que el Ecuador use sustentablemente sus recursos naturales estratégicos para alcanzar el Buen vivir.

Objetivos

- ✓ Incorporar los costos y beneficios ambientales y sociales en los indicadores económicos, que permitan priorizar actividades productivas de menos impacto y establecer mecanismos de incentivo adecuados.
- ✓ Generar información sobre la oferta de recursos naturales estratégicos renovables por ecosistema para su manejo integra

- ✓ Reducir la vulnerabilidad ambiental, social y económica frente al cambio climático, concienciar a la población sobre causas y efectos de este fenómeno antropogénico y fomentar la reducción de las emisiones de gases de efecto invernadero en los sectores productivos y sociales.
- ✓ Reducir el consumo de recursos (electricidad, agua y papel) y de producción de desechos.
- ✓ Manejar la conflictividad socio ambiental a través de la incorporación de los enfoques de la participación ciudadana, e interculturalidad y/o género en los proyectos de gestión ambiental.
- ✓ Definir y determinar información e investigación válidas y pertinentes para mejorar la gobernanza ambiental en los ámbitos de la normativa, la dinámica internacional y la participación ciudadana.
- ✓ Fortalecer la institucionalidad del Ministerio del Ambiente.

Valores

- **Legalidad:** los funcionarios y funcionarias, servidores y servidoras públicos del Ministerio del Ambiente trabajarán en forma responsable y conforme los lineamientos, normas, políticas reglamentos y disposiciones legales, sin favorecer ni perjudicar a nadie de manera injusta.
- **Rendición de cuentas:** todos los funcionarios y funcionarias, servidores y servidoras públicos del Ministerio del Ambiente deben informar y documentar sus actividades y decisiones, aceptando e incluso facilitando la revisión, análisis y evaluación de sus acciones y resultados.
- **Calidad:** todos los funcionarios y funcionarias, servidores y servidoras públicos del Ministerio del Ambiente deben preocuparse por exceder los requerimientos y necesidades de sus clientes externos e internos.
- **Compromiso**: lograr el compromiso de todos los actores involucrados, así como la apropiación de responsabilidades en las acciones determinadas en el Plan Estratégico.
- **Relevancia:** destacar que la nueva visión del ministerio del ambiente evocada en el manejo sustentable de los ecosistemas, tiene un importante impacto en garantizar los derechos de la naturaleza y promover un ambiente sano y sustentable.

- **Participación:** promover la participación de los funcionarios del MAE, integrando al proceso a todos los involucrados (funcionarios del Ministerio de Planta Central y de Coordinaciones generales Zonales y Direcciones Provinciales).
- **Académico:** tener presente para la implementación de los equipos funcionales los aportes académicos con base epistemológica sólida y reconocida.

Capitulo II

RESULTADO DEL EXAMEN

- ***SEGURIDAD LÓGICA***

FALTA DE POLÍTICAS Y PROCEDIMIENTOS.

En la Dirección Provincial del MAE PASTAZA no se promueven ni se establecen políticas y procedimientos que normen las actividades de la unidad de tecnologías de Información.

RECOMENDACIÓN 01: AL DIRECTOR PROVINCIAL Y FUNCIONARIO DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Promoverá y establecerá políticas y procedimientos que regulen las actividades relacionadas con las Tecnologías de Información, acatando y aplicando la Norma de Control Interno 410-04, que concierne a "*Políticas y Procedimientos*, estableciendo así un adecuado control y lineamientos dentro de todas las actividades que se desarrollan en la unidad de Tecnologías de Información del MAE-PASTAZA, de este modo salvaguardar los datos, información y equipos Informáticos que posee la institución.

FALTA DE CONTROL PARA SITIOS WEB.

En la Dirección Provincial del MAE-PASTAZA no se establece normas, procedimiento e instructivos de instalación, configuración, y utilización de los servicios de internet, correos electrónicos y sitios WEB de la entidad.

RECOMENDACIÓN 02: AL FUNCIONARIO DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Establecerá normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, correos electrónicos, y sitos WEB de la entidad, acatando y aplicando la Norma de Control Interno 410-14, que concierne a "*Sitios web, servicios de internet e intranet.*", evitando daños parciales o totales a los equipos informáticos, así como también fuga y/o pérdida de información propia de la institución.

- ***SEGURIDAD FÍSICA***

INEXISTENCIA DE MECANISMOS DE SEGURIDAD.

En la dirección provincial del MAE PASTAZA no se establecen los mecanismos necesarios que salvaguarden los medios Informáticos existentes en la unidad de tecnologías de información.

RECOMENDACIÓN 03: AL FUNCIONARIO DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN.

Establecerá los mecanismos de seguridad necesarios que ayuden a salvaguardar los medios Informática de la institución, acatando y aplicando la Norma de Control Interno 410-10, que concierne a "*Seguridad de Tecnologías de Información*", evitando así pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos existente en la institución.

INEXISTENCIA DE PLANES DE CONTINGENCIA.

En la Dirección Provincial del MAE-PASTAZA No definen planes de contingencia para que sean ejecutados en casos de emergencias que se susciten en la institución y afecten directa o indirectamente a la unidad de tecnologías de información.

RECOMENDACIÓN 04: AL FUNCIONARIO ENCARGADO DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Definirá planes de contingencias donde se describan los lineamientos a seguir en caso de emergencias suscitadas dentro de la institución, acatando y aplicando la Norma de Control Interno 410-11, que concierne a "*Plan de contingencias*", para una adecuada toma de decisiones en caso de emergencias o problemas presentados en equipos, instalaciones o personal relacionado, que desemboca en pérdidas de información y operatividad de la unidad.

- ***GESTIÓN INFORMÁTICA***

FALTA DE IDENTIFICACIÓN DE LA UNIDAD INFORMÁTICA.

En la Dirección Provincial del MAE-PASTAZA no se identificar dentro de su estructura organizacional a la unidad de Tecnologías de Información.

RECOMENDACIÓN 05: AL DIRECTOR, FUNCIONARIO ENCARGADO DE LA UNIDAD DE TECNOLOGÍAS DE INFORMÁTICAS.

Gestionará e identificará dentro de su estructura organizacional en un nivel de apoyo a la unidad de Tecnologías de Información, acatando y aplicando Norma de Control Interno 410-01, que concierne a "*Organización Informática*", para facilitar la transparencia, estandarización y control de las Tecnologías de Información del MAE-PASTAZA.

INEXISTENCIA DE PLANES DE MANTENIMIENTO Y CONTROL DE INVENTARIO.

En la Dirección Provincial del MAE-PASTAZA no se elabora y aplica Planes de mantenimiento correctivo/preventivo, así como también el control de inventario de los bienes existentes en la unidad de tecnologías de información.

RECOMENDACIÓN 06: AL FUNCIONARIO RESPONSABLE DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN.

Desarrollará y ejecutará planes de mantenimiento para toda la infraestructura tecnológica, así como también levantar un inventario de los bienes existentes en la institución, acatando y aplicando la Norma de Control Interno 410-09, que concierne a "*Mantenimiento y control de la infraestructura tecnológica*", evitando así daños parciales o totales de la infraestructura tecnológica, pérdida de recursos, datos erróneos e inexactos en la existencia y control de bienes.

INEXISTENCIA DE MONITOREO Y EVALUACIÓN DE PROCESOS.

En la Dirección Provincial del MAE-PASTAZA no existen sistemas de monitoreo y evaluación a los procesos operativos de la unidad de tecnologías de información.

RECOMENDACIÓN 07: AL FUNCIONARIO RESPONSABLE DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN.

Definirá y ejecutará sistemas de monitoreo y evaluación donde se determine el grado de operatividad de la unidad Tecnológica de la institución, acatando y aplicando la Norma de Control Interno 410-13, que concierne a "*Monitoreo y evaluación de los procesos y servicios.*", con el propósito de detectar y corregir deficiencias operativas en la unidad de tecnologías de información, aportando así a la consecución de metas y objetivos planteados por la institución.

FALTA DE CAPACITACIÓN INFORMÁTICA.

En la Dirección Provincial del MAE-PASTAZA no existe el debido desarrollo y ejecución de planes de capacitación tanto a usuarios internos como externos de la unidad de tecnologías de la información.

RECOMENDACIÓN 08: AL DIRECTOR Y FUNCIONARIO DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Desarrollarán y ejecutarán planes de capacitación donde se integre a todos los usuarios directos e indirectos de las tecnologías de información de la institución, acatando y aplicando la Norma de Control Interno 410-15, que concierne a "*Capacitación Informática.*", conservando así el estado físico de la infraestructura tecnológica y la integridad de la información.

4.3 VERIFICACIÓN DE LA IDEA A DEFENDER

General

La Idea plantea dentro del siguiente trabajo es, "*La Auditoria Informática de las Tecnologías de Información y Comunicación en la Dirección Provincial del ambiente de Pastaza, período 2013, comprobará que no se está dando cumplimiento a las normas y leyes establecidas*", una vez finalizado el examen al área informática del MAE-PASTAZA se concluye y analiza los resultados obtenidos a lo largo de todo el desarrollo de la auditoria Informativa y se obtiene una Idea VERDADERA, es decir que en la Dirección Provincial del MAE-PASTAZA no se está dando cumplimiento en cuanto a la aplicación de las Normas de Control interno Emitidas Por la Contraloría General del Estado puntual mente el grupo de las 400, subgrupo 410 referente a las tecnologías de información y comunicación.

Específicas

Así también se AFIRMAN las Ideas especificas ya que los procesos de administración, uso y manejo de las tic´s son incorrectas.

Se AFIRMA que la vulnerabilidad de la información se encuentra ampliamente comprometida.

Se AFIRMA que la emisión del informe ayudara a corregir errores detectados.

CONCLUSIONES

- Mediante la realización de la Auditoría Informática se detectaron deficiencias en cuanto al cumplimiento de Normas de Control Interno emitidas por la Contraloría General del Estado, por lo que, se emite comentarios, conclusiones y recomendaciones para cada una de las deficiencias encontradas con miras a un mejoramiento constante para un adecuado desarrollo de las actividades diarias llevadas en la unidad de Tecnologías de Información de la Dirección Provincial del MAE-PASTAZA.

- La Dirección Provincial del MAE-PASTAZA no cuenta con una Unidad de Tecnologías de Información debidamente identificada dentro de su Estructura Orgánica según lo dispone la Norma de Control Interno 410-01 referente a "*Organización Informática",* por lo que, el Director debe promover e identificar a dicha unidad dentro de su estructura organizacional en un nivel de apoyo o asesoría.

- La institución no desarrolla y aplica políticas y procedimientos que regulen las actividades relacionadas con las Tecnologías de Información, conforme dispone la Norma de Control Interno 410-04, referente a "*Políticas y Procedimientos*.

- La Dirección Provincial del MAE-PASTAZA no elabora y aplica Planes de mantenimiento correctivo/preventivo, así como también no existe un control de inventario de los bienes existentes en la unidad de tecnologías de información según lo dispone la Norma de Control Interno 410-09, referente a "*Mantenimiento y control de la infraestructura tecnológica*".

- La Dirección Provincial del MAE PASTAZA no determina los mecanismos de seguridad necesarios que salvaguarden los medios Informáticos existentes en la unidad de tecnologías de información según lo dispone la Norma de Control Interno 410-10, referente a "*Seguridad de Tecnologías de Información*".

- La Institución del no define planes de contingencia para que sean ejecutados en casos de emergencias que se susciten en la institución y afecten directa o indirectamente a la unidad de tecnologías de información según lo dispone la Norma de Control Interno 410-11, referente a "*Plan de contingencias*".

- La Dirección Provincial del MAE-PASTAZA no desarrolla sistemas de monitoreo y evaluación a los procesos operativos de la unidad de tecnologías de información según lo establece la Norma de Control Interno 410-13, referente a "*Monitoreo y evaluación de los procesos y servicios.*"

- La Dirección Provincial del MAE-PASTAZA no establece normas, procedimiento e instructivos de instalación, configuración, y utilización de los servicios de internet, correos electrónicos y sitios WEB de la entidad según lo establece la Norma de Control Interno 410-14, referente a "*Sitios web, servicios de internet e intranet.*"

- La Dirección Provincial del MAE-PASTAZA no desarrolla y ejecuta planes de capacitación tanto a usuarios internos como externos de la unidad de tecnologías de la información según lo establece la Norma de Control Interno 410-15, referente a "*Capacitación Informática.*"

RECOMENDACIONES

- Se considera que los funcionarios de la Dirección Provincial del MAE-PASTAZA tomen en consideración el informe de Auditoría Informática el cual incluye conclusiones y recomendaciones en cuanto a la aplicación de normas y leyes.

- El Director conjuntamente con el funcionario encargado de la unidad de Tecnologías de información deben gestionar e identificar dentro de la estructura organizacional en un nivel de apoyo a la unidad de Tecnologías de Información, para facilitar la transparencia, estandarización y control de las Tecnologías de Información del MAE-PASTAZA.

- El Director Provincial en coordinación con el funcionarios de la unidad de tecnologías de información deben promover y establecer políticas y procedimientos que regulen las actividades relacionadas con las Tecnologías de Información, garantizando así un adecuado control y lineamientos dentro de todas las actividades que se desarrollan en la unidad de Tecnologías de Información del MAE-PASTAZA.

- El Funcionario responsable de la unidad de tecnologías de información desarrollara y ejecutara planes de mantenimiento para toda la infraestructura tecnológica, así como también levantar un inventario de los bienes existentes en la institución, con el propósito de evitar daños parciales o totales de la infraestructura tecnológica, pérdida de recursos y contar con datos precisos y exactos de la existencia de bienes.

- El encargado de la unidad informática debe establecer los mecanismos de seguridad necesarios que ayuden a salvaguardar los medios informáticos de la institución, para evitar así pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos existente en la institución.

- El funcionario encargado de la unidad de tecnologías de información debe definir y ejecutar planes de contingencias donde se describan los lineamientos a seguir en caso de emergencia suscitadas dentro de la institución, garantizando

así una adecuada toma de decisiones en caso de emergencias o problemas presentados en equipos, instalaciones o personal relacionado.

- El funcionario de la unidad tecnológica debe definir y ejecutar sistemas de monitoreo y evaluación donde se determine el grado de operatividad de la unidad Tecnológica de la institución con el propósito de detectar y corregir deficiencias operativas en la unidad de tecnologías de información.

- El funcionario encargado del a unidad informática debe establecer normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, correos electrónicos, y sitos WEB de la entidad, para evitar así daños parciales o totales de los equipos informáticos, así como también fuga y/o pérdida de información propia de la institución.

- El Director en coordinación del funcionario encargado de la unidad tecnológica deberán desarrollar y ejecutar planes de capacitación donde se integre a todos los usuarios directos e indirectos de las tecnologías de información de la institución, conservando así el estado físico de la infraestructura tecnológica y la integridad de la información.

BIBLIOGRAFÍA

- Estupiñan Gaitán, R. (2006). *Control Interno y fraudes con base los ciclos transaccionales: Análisis del Informa COSO I y II, 2a ed.* Bogotá: Coe Ediciones.
- Franklin, B. (2007). *Auditoría Administrativa: Gestión Estrategica del cambio, 2a ed.* México: Pearson Educación.
- Franklin, B. (2013). *Auditoria Administrativa: Evaluación y Diagnostico Empresarial, 3a ed.* México: Pearson Educación.
- Mantilla, S. (2008). *Control Interno COSO, 2a ed.* Bogotá: Coe Ediciones.
- Muñoz Raso, C. (2002). *Auditoría en Sistemas Computacionales.* México: Pearson Educación.
- Piattini, M., & Del Poso, E. (2008). *Auditoría Informatica: Un enfoque práctico, 2a ed.* México: Alfaomega.

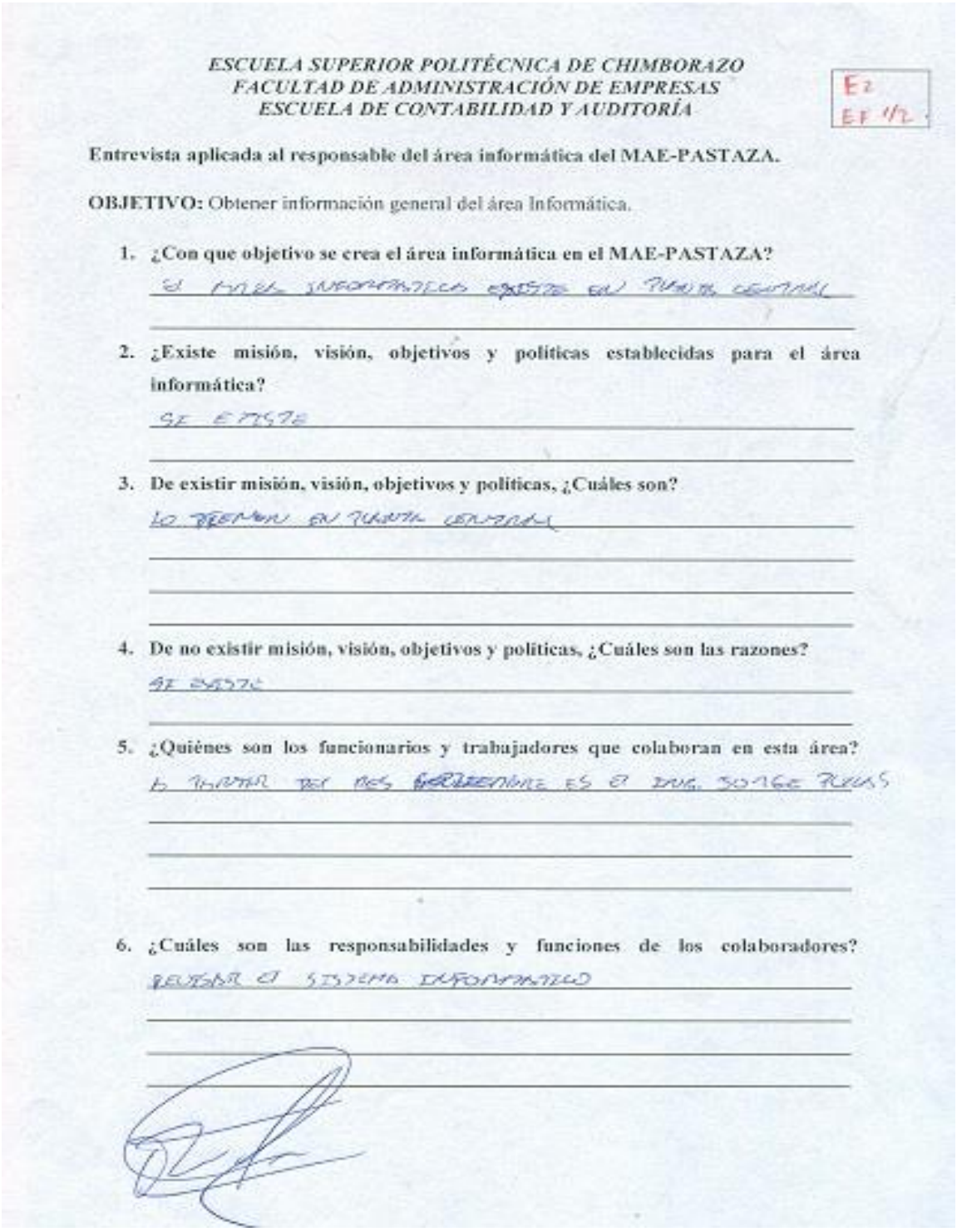
LINKOGRAFÍA

- Carchi, L. (8 de Mayo de 2013). *Importancia de la Auditoría Informatica*. (Recuperado 2014-11-30) de http://carchililia.blogspot.com
- Contraloria General del Estado. (16 de 11 de 2009). *Normas de control Interno para las entidades, organismos del sector público y de las personas juridicas de derecho privado que dispongan de recursos públicos*. (Recuperado 2014-10-28) de http://www.contraloria.gob.ec/documentos/normatividad
- Farinango Alvear, V. (Marzo de 2012). *Auditoría de Gestión para Evaluar el Cumplimiento de los Proyectos de obras Públicas en el Gobierno Municipal de Cayambe del Periodo 2010 (Tesis de ingenieria, Universidad Central del Ecuador).* (Recuperado 2015-06-10) de http://www.dspace.uce.edu.ec/bitstream/25000/617/1/T-UCE-0003-27.pdf
- Ministerio del Ambiente. (s.f.). *Cultura organizacional*. (Recuperado 2014-09-25) de http://www.ambiente.gob.ec/el-ministerio/

ANEXOS

ANEXO 1: PAPELES DE TRABAJO

- **ENCUESTA APLICADA AL DIRECTOR PROVINCIAL DEL MAE-PASTAZA**



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

E2
EF 1/2

Entrevista aplicada al responsable del área informática del MAE-PASTAZA.

OBJETIVO: Obtener información general del área Informática.

1. **¿Con que objetivo se crea el área informática en el MAE-PASTAZA?**
   EL AREA INFORMATICA EXISTE EN TODA CENTRAL
2. **¿Existe misión, visión, objetivos y políticas establecidas para el área informática?**
   SE EXISTE
3. **De existir misión, visión, objetivos y políticas, ¿Cuáles son?**
   LO PRIMERO EN TODA CENTRAL
4. **De no existir misión, visión, objetivos y políticas, ¿Cuáles son las razones?**
   SE EXISTE
5. **¿Quiénes son los funcionarios y trabajadores que colaboran en esta área?**
   EL TUTOR DEL DOS PRIMEROS ES EL ING. JORGE RUIZ
6. **¿Cuáles son las responsabilidades y funciones de los colaboradores?**
   REVISAR EL SISTEMA INFORMATICO

ENCUESTA APLICADA AL FUNCIONARIO ENCARGADO DE LA UNIDAD INFORMÁTICA

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

EL
EF 1/2

Entrevista aplicada al responsable del área informática del MAE-PASTAZA.

OBJETIVO: Obtener información general del área Informática.

1. **¿Con que objetivo se crea el área informática en el MAE-PASTAZA?**
   DAR SOPORTE DE PRIMER NIVEL PARA LA DIRECCION PROVINCIAL DESCENTRALIZADO
2. **¿Existe misión, visión, objetivos y políticas establecidas para el área informática?**
   SI, PERO ES LA MISMA DEL MINISTERIO DEL AMBIENTE
3. **De existir misión, visión, objetivos y políticas, ¿Cuáles son?**
   APARTE DE LA MISIÓN Y VISION DEL MAE EXISTEN POLITICAS COMO SEGURIDAD DE LA INFORMACION, ACUERDOS DE SEGURIDAD INFORMÁTICA, ENTRE OTROS.
4. **De no existir misión, visión, objetivos y políticas, ¿Cuáles son las razones?**
   —
5. **¿Quiénes son los funcionarios y trabajadores que colaboran en esta área?**
   - DIRECTOR DE T.I. (ING. MARCELO SARMIENTO)
   - ANALISTAS DE SEGURIDAD
   - ESPECIALISTAS EN INFRAESTRUCTURA
   - SOPORTE TECNICO
6. **¿Cuáles son las responsabilidades y funciones de los colaboradores?**
   - VELAR POR EL FUNCIONAMIENTO, USO, SEGURIDAD Y CONTROL DE LA T.I. DEL MINISTERIO

TECNICO T.
MAE-PAST

- **CUESTIONARIOS DE CONTROL INTERNO**

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

E.S.C.C.I.S.L

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoría:	Auditoría Informática
Componente:	Seguridad Lógica
Objetivo:	Verificar la existencia y aplicación de las medidas para contrarrestar las amenazas que pueda afectar la integridad de los datos e información de la entidad.

N°	PREGUNTAS	RESPUESTAS SI	NO	N/A	OBSERVACIONES
1	¿El sistema operativo de los ordenadores cumple con las características necesarias para el desarrollo de las actividades?	X			
2	¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?		X		
3	¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal?	X			
4	¿Existen procedimientos de notificación y gestión de incidencias?		X		
5	¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos e información?				
6	¿Existe personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?	X			
7	¿Se realizan controles periódicos para verificar el cumplimiento de procesos y normas?		X		
8	¿Existen medidas y/o procedimiento a adoptar cuando se agregue o suprime aplicaciones y/o software que modifique parcial o total los ordenadores?	X			
9	¿Se restringe el acceso a personal no autorizado a acceder a las instalaciones donde se encuentren ubicados los sistemas informáticos que guardan información de la institución?	X			
10	¿Se restringe el acceso a ordenadores donde se guarda el soporte de datos e información?	X			
11	¿Existe un periodo máximo caducidad de las contraseñas de acceso?	X			
12	¿Existe una clasificación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos?	X			
13	12. ¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas, y las mismas están debidamente documentadas?		X		
14	¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?	X			
15	¿En el sistema están habilitadas para todas las cuentas de usuario las opciones que permiten establecer: • Un número máximo de intentos de conexión. • Un periodo máximo de vigencia para la contraseña.	X			
16	¿Existen procedimientos de asignación y distribución de contraseñas?	X			
17	¿Se realizan auditorías a los archivos de seguridad?		X		
TOTAL					

Elaborado por:	C.L.C.H	Fecha:	09/12/14
Revisado por:	A.G.L.P.	Fecha:	10/12/14

TECNICO - MAE PAAS

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

C.C. I
SF 1/2

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoria:	Auditoria Informática
Componente:	Seguridad Física
Objetivo:	Revisar las políticas y Normas sobre seguridad Física, seguridad de personal, datos, hardware, software e instalaciones.

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Se han adoptado medidas de seguridad para salvaguardar los sistemas de información?	X			
2	¿Existe una persona responsable de la seguridad?	X			
3	¿Existe personal de vigilancia en la institución?	X			
4	¿Se investiga a los vigilantes cuando son contratados?	X			
5	¿Existe vigilancia en las instalaciones las 24 horas?	X			
6	¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?	X			
7	¿Se registra el acceso al área informática de personas ajenas a la dirección?		X		
8	¿Se vigilan la moral y comportamiento del personal con el fin de mantener una buena imagen y evitar un posible fraude?		X		
9	¿Existe un sistema de ventilación adecuado para los equipos e instalaciones?		X		
10	¿Existen extintores de fuego en las instalaciones?	X			
11	¿Se ha capacita y entrenado al personal en el manejo de los extintores?	X			
12	¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstrucciones?	X			
13	¿El personal saben que hacer en caso de que ocurra una emergencia ocasionado por fuego?	X			
14	¿El personal ajeno a operación sabe qué hacer en el caso de un incendio?	X			
15	¿Existe salida de emergencia?	X			
16	¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas?		X		
17	¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior de las instalaciones a fin evitar daños a los equipos?	X			
18	¿Se limpia con frecuencia el polvo acumulado en lugares de difícil acceso para evitar daños a los equipos?	X			
19	¿Existen procedimientos para la realización de las copias de seguridad?		X		
20	¿Hay procedimientos que aseguran la realización de copias de todos aquellos datos que han experimentado algún cambio en su contenido?	X			
21	¿Existen controles sobre el acceso físico a las copias de seguridad?	X			

TÉCNICO I.
MAE-PAS

C.C.I
S.F 2/2

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

22	¿Existe un inventario de los soportes existentes?	X			
23	¿Dicho inventario incluye las copias de seguridad?	X			
24	¿Existen procedimientos de etiquetado e identificación del contenido de los soportes?	X			
25	¿Se Verifica que todos los soportes cuenten con claves de acceso?	X			
TOTAL					

Elaborado por:	C.L.C.M	Fecha:	05/12/13
Revisado por:	A.G.I.P	Fecha:	06/01/14

TECNICO I.
MAE-NRAS

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

C.C.I
T.I

DE CONTROL INTERNO

CUESTIONARIO DE INVESTIGACIÓN	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoría:	Auditoría Informática
Componente:	Tecnologías de Información
Objetivo:	Conocer aspectos relacionados a la utilización y aprovechamiento de los recursos informáticos a fin de determinar si los equipos disponibles son actualizados y si existen políticas establecidas para su utilización.

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existe un plan logístico para el mantenimiento preventivo/correctivo del software?	X			
2	¿Existe un plan logístico para el mantenimiento preventivo/correctivo para el hardware e instalaciones?	X			
3	¿Los planes de mantenimiento se cumplen a cabalidad?		X		
4	¿Existen procedimientos para solucionar daños o fallas existentes en los equipos?	X			
5	¿Existe tiempos establecidos para la solución de problemas presentados en los equipos?	X			
6	¿Se mantienen planes de limpieza adecuados a fin de evitar la acumulación de polvo en los equipos?	X			
7	¿Los equipos existentes son suficientes para la operatividad de la institución?	X			
8	¿Existe suficiente mobiliario para la operatividad y desenvolvimiento de los sistemas informáticos?		X		
9	¿Existen políticas que norme el trabajo definidas del personal que labora en esta área?	X			
10	¿Existe políticas, manuales y procesos de utilización y uso de los equipos informáticos?		X		
11	¿El software (programas) disponibles en los ordenadores de la institución contribuyan a las actividades diarias de la misma?	X			
12	¿Existe software ofimática (programas y herramientas informáticas de oficina) actualizado que estén disponibles para los empleados y funcionarios de la institución?	X			
13	¿Existe software utilitario que sea de apoyo y que estén disponibles para los empleados y funcionarios?	X			
14	¿La información transmitida por internet es controlada?	X			
15	¿Se elabora normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitios WEB en base a las disposiciones legales?		X		
16	¿Se considera el desarrollo de aplicaciones WEB y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general?	X			
17	¿El servicio de Internet satisface las necesidades de la institución?	X			
TOTAL					

Elaborado por:	C.C.M	Fecha:	05/12/
Revisado por:	A.G.P	Fecha:	06/12/

TECNICO I.
MAE - PAS

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

C.C.I
6I

CUESTIONARIO

Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoria:	Auditoría Informática
Componente:	Gestión Informática
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Se desarrolla regularmente planes a corto, medio y largo plazo que apoyen el logro de la misión, visión y metas de la institución?	X			
2	¿Dispone la institución de un plan Estratégico de Tecnología de Información?	X			
3	¿La planificación del área informática, está en función del plan estratégico de toda la institución?	X			
4	¿Las tareas y actividades plasmadas en el plan tienen la correspondiente y adecuada asignación de recursos?	X			
5	¿Existe un comité de informática?		X		
6	¿Existen estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y actualizados?	X			
7	¿Las descripciones de los puestos de trabajo reflejan las actividades realizadas en la práctica?	X			
8	¿Existen controles que tienden a asegurar que el cambio de puesto de trabajo y la finalización de los contratos laborales no afectan a los controles internos y a la seguridad informática?	X			
9	¿Existe un presupuesto económico para la adquisición de nuevos bienes? ¿Y hay un proceso para elaborarlo?	X			
10	¿Existen procedimientos para la adquisición de bienes y servicios?		X		
11	¿Existe un plan operativo anual?		X		
12	¿Existe un cronograma de cumplimiento de metas?		X		
13	¿Se comprueban los resultados con datos reales?		X		
14	¿Existe un organigrama con la estructura de organización del área?		X		
15	¿El presupuesto está en concordancia con los objetivos a cumplir?	X			
16	¿Existen procedimientos para vigilar y determinar permanentemente la normativa aplicable?		X		
TOTAL					

Elaborado por:	C.L.C.M	Fecha:	05/12/11
Revisado por:	A.G.I.P.	Fecha:	07/12/11

TECNICO I.
MAE-PAAS

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

C C I
ADM 3/8

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoría:	Auditoría Informática
Componente:	Administración/usuarios
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?		X		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?		X		
4	¿Existen procedimientos adecuados para mantener la documentación al día?	✓			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	✓			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	✓			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?		X		
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	✓			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?		X		
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	✓			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	✓			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	✓			
TOTAL					

Elaborado por:	C L C M	Fecha:	09/12/14
Revisado por:	A C P	Fecha:	06/14/14

CRISTHIAN GAECON

ANALISTA DE TALENTO HUMA
MAE - PASTAZA.

DIRECCION PROVINCIAL DEL AMBIENTE DE PASTAZA
Ministerio del Ambiente
RECURSOS HUMANOS

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

C C E
ADM 9/8

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoría:	Auditoría Informática
Componente:	Administración/usuarios
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?		X		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	X			
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?		X		
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	X			
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL					

Elaborado por:	C.L.C.H	Fecha:	oct/15
Revisado por:	A.G.I.P	Fecha:	oct/15

Especialista de la Unidad de Calidad Ambiental

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

CCI
ADM 6/8

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoría:	Auditoría Informática
Componente:	Administración/usuarios
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática

Nº	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?		X		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?		X		
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?		X		
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?		X		
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	X			
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?			X	
TOTAL					

Elaborado por:	C L C H	Fecha:	octubre
Revisado por:	A G I P	Fecha:	06/11/09

ADMINISTRADORA.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

C.C.I
A.01.2.8

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoría:	Auditoría Informática
Componente:	Administración/usuarios
Objetivo:	Verificar procedimientos aplicados a la gestion que se realiza en el área informática.

N°	PREGUNTAS	RESPUESTAS SI	NO	N/A	OBSERVACIONES
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?	✓			
2	¿Se aprueban solicitudes de nuevas aplicaciones?	✓			
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	✓			
4	¿Existen procedimientos adecuados para mantener la documentación al día?	✓			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	✓			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	✓			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	✓			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	✓			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?		X		
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	✓			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	✓			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	✓			
TOTAL					

Elaborado por:	C.C.C.M	Fecha:	07/12/18
Revisado por:	A.G.P	Fecha:	07/12/18

ESPECIALISTA AMBIENTAL .

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

C.C.I
AGH 1/8

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoria:	Auditoria Informática
Componente:	Administración/usuarios
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.

Nº	PREGUNTAS	RESPUESTAS SI	NO	N/A	OBSERVACIONES
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?	X			
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?		X		
4	¿Existen procedimientos adecuados para mantener la documentación al día?		X		
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	X			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?		X		
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL					

Elaborado por:	C.C	Fecha:	05/12/19
Revisado por:	AGIP	Fecha:	06/12/19

Asist. Jurídico.
CI. 1600517070

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

CCI
ADM 5/8

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Area evaluada:	Informática/Tecnológica
Tipo de Auditoria:	Auditoria Informática
Componente:	Administración/usuarios
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.

Nº	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?	X			
2	¿Se aprueban solicitudes de nuevas aplicaciones?	X			
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	X			
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	X			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	X			
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	X			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL					

Elaborado por:	C.L.C.M	Fecha:	05/12/19
Revisado por:	A.G.I.P	Fecha:	10/12/19

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

CCI
ADM 7/8

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoría:	Auditoría Informática
Componente:	Administración/usuarios Secretaria
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.

N°	PREGUNTAS	RESPUESTAS SI	NO	N/A	OBSERVACIONES
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?	/			
2	¿Se aprueban solicitudes de nuevas aplicaciones?		/		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?		/		
4	¿Existen procedimientos adecuados para mantener la documentación al día?	/			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?		/		
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	/			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	/			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	/			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?		/		
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	/			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	/			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	/			
TOTAL					

Elaborado por:	C.L.C.M	Fecha:	05/12/14
Revisado por:	A.C.I.P	Fecha:	08/12/14

Secretaria

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE ADMINISTRACIÓN DE EMPRESAS
ESCUELA DE CONTABILIDAD Y AUDITORÍA

CCI
ADM 8/8

CUESTIONARIO	
Entidad:	Dirección Provincial del MAE-PASTAZA
Área evaluada:	Informática/Tecnológica
Tipo de Auditoría:	Auditoría Informática
Componente:	Administración/usuarios Coordinador Patrimonio Cultural
Objetivo:	Verificar procedimientos aplicados a la gestión que se realiza en el área Informática.

N°	PREGUNTAS	RESPUESTAS			OBSERVACIONES
		SI	NO	N/A	
1	¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?		X		
2	¿Se aprueban solicitudes de nuevas aplicaciones?		/		
3	¿Existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	X			
4	¿Existen procedimientos adecuados para mantener la documentación al día?	X			
5	¿Se aprueban los programas nuevos y se revisan antes de ponerlos en funcionamiento?	X			
6	Por fallos de hardware, software o electricidad. ¿Se puede garantizar la integridad y confiabilidad de los datos e información de los sistemas?	X			
7	¿Existe las seguridades adecuadas para evitar daños o alteraciones en el sistema por terceras personas?	X			
8	¿Dentro del desarrollo de actividades realiza usted respaldos de la información generada?	X			
9	¿Existen procedimientos establecidas para la eliminación de archivos en caso de no considerarlos necesarios para el desarrollo de actividades?	X			
10	¿Considera usted que el sistema que utiliza es adecuado para el desarrollo de actividades?	X			
11	¿Se tiene establecido políticas de cambio de claves de acceso durante un determinado tiempo?	/			
12	En caso de no existir dichas políticas ¿Considera usted que es importante realizar cambios de claves de acceso en los sistemas, dentro de un determinado tiempo por motivos de seguridad?	X			
TOTAL					

Elaborado por:	C L C M	Fecha:	05/12/14
Revisado por:	A G I P	Fecha:	05/12/14

Coordinador de Patrimonio Cultural
05-12-2014.

ANEXO 2: MANUAL DE FUNCIONES

DESCRIPCIÓN Y PERFIL DE PUESTOS
MINISTERIO DEL AMBIENTE

1. DATOS DE IDENTIFICACION DEL PUESTO		4. RELACIONES INTERNAS Y EXTERNAS	5. INSTRUCCIÓN FORMAL REQUERIDA	
Codigo:	1.10.01.5.3.01.05.02.1	INTERFAZ		
Denominación:	Analista de Tecnologías provincial	Funcionarios del MAE, Unidades Administrativas	Instrucción:	Tercer nivel
Nivel:	Profesional		Título Requerido:	Ingeniería
Unidad o Proceso:	Direccion Provincial del Ambiente		Area de Conocimiento:	Informática,Sistemas, Comunicaciones
Rol:	Ejecución de Procesos			
Grupo Ocupacional:	Servidor Publico 2			
Grado:	8			
Nivel de Aplicación:	Ambito Nacional			

2. MISION	6. EXPERIENCIA LABORAL REQUERIDA	
Ejecutar actividades de desarrollo y mantenimiento de software de forma sistemática y productiva, asegurando su calidad, fiabilidad y facilidad de uso de los sistemas informáticos, tecnologías de la información y comunicaciones.	Tiempo de Experiencia:	1 año
	Especificidad de la experiencia:	Herramientas de desarrollo basados en software libre Ofimática Base de datos Auditoria Seguridad Tecnológica Sistemas operativos Arquitectura de aplicaciones

3. ACTIVIDADES ESENCIALES	7. CONOCIMIENTOS	8. DESTREZAS
Controla mecanismos de seguridades en los sistemas automatizados, accesos, bases de datos, redes y comunicaciones.	Seguridad informática y tecnológica, Manejo de base de datos y herramientas de ingeniería de software, Administración de usuarios, Normas y Acuerdos técnicos, Análisis y diseño de sistemas requeridos, Desarrolla e implementación de sistemas de información y tecnológicos	Orientación / asesoramiento
Administra y mantiene los usuarios de los sistemas de información	Seguridad informática y tecnológica, Manejo de base de datos y herramientas de ingeniería de software, Administración de usuarios, Normas y Acuerdos técnicos, Análisis y diseño de sistemas requeridos, Desarrolla e implementación de sistemas de información y tecnológicos	Planificación y gestión
Brinda soporte del mantenimiento de los sistemas informáticos que apoyan a diferentes Unidades o Direcciones del Ministerio	Seguridad informática y tecnológica, Manejo de base de datos y herramientas de ingeniería de software, Administración de usuarios, Normas y Acuerdos técnicos, Análisis y diseño de sistemas requeridos, Desarrolla e implementación de sistemas de información y tecnológicos	Operación y control
Elabora y ejecuta programas de capacitación de los sistemas informáticos y tecnológicos a los servidores de la institución para que pueda ejecutarlos y operarlos en forma segura y adecuada	Seguridad informática y tecnológica, Manejo de base de datos y herramientas de ingeniería de software, Administración de usuarios, Normas y Acuerdos técnicos, Análisis y diseño de sistemas requeridos, Desarrolla e implementación de sistemas de información y tecnológicos	Generación de ideas
Mantiene actualizada y en custodia la documentación técnica y del usuario de los sistemas de información en operación	Seguridad informática y tecnológica, Manejo de base de datos y herramientas de ingeniería de software, Administración de usuarios, Normas y Acuerdos técnicos, Análisis y diseño de sistemas requeridos, Desarrolla e implementación de sistemas de información y tecnológicos	Análisis de operaciones
Administra redes de comunicación, correo electrónico, internet, base de datos, y otros servicios instalados.	Administración del cableado estructurado, Seguridad informática y tecnológica, Instalación y configuración básica de la infraestructura de las redes de comunicación e información, Análisis y diseño de sistemas, Administración de	Diseño de tecnología
Realiza cableado y equipos que conforman la infraestructura básica de la red informática del MAE	Administración del cableado estructurado, Seguridad informática y tecnológica, Instalación y configuración básica de la infraestructura de las redes de comunicación e información, Análisis y diseño de sistemas, Administración de	Mantenimiento de equipos
Verifica el mantenimiento y actualización del sitio Web institucional.	Administración del cableado estructurado, Seguridad informática y tecnológica, Instalación y configuración básica de la infraestructura de las redes de comunicación e información, Análisis y diseño de sistemas, Administración de proyectos y tendencias tecnológicas	Diseño de tecnologías

142

ANEXO 3: NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS410 TECNOLOGÍA DE LA INFORMACIÓN

410-01 Organización informática

Las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección, por lo que las actividades y procesos de tecnología de información de la organización deben estar bajo la responsabilidad de una unidad que se encargue de regular y estandarizar los temas tecnológicos a nivel institucional.

La unidad de tecnología de información, estará posicionada dentro de la estructura organizacional de la entidad en un nivel que le permita efectuar las actividades de asesoría y apoyo a la alta dirección y unidades usuarias; así como participar en la toma de decisiones de la organización y generar cambios de mejora tecnológica. Además debe garantizar su independencia respecto de las áreas usuarias y asegurar la cobertura de servicios a todas las unidades de la entidad u organismo.

Las entidades u organismos del sector público, establecerán una estructura organizacional de tecnología de información que refleje las necesidades institucionales, la cual debe ser revisada de forma periódica para ajustar las estrategias internas que permitan satisfacer los objetivos planteados y soporten los avances tecnológicos. Bajo este esquema se dispondrá como mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica y soporte interno y externo de ser el caso, considerando el tamaño de la entidad y de la unidad de tecnología.

410-02 Segregación de funciones

Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.

La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal.

La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave.

410–03 Plan informático estratégico de tecnología

La unidad de tecnología de la información elaborará e implementará un plan informático estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el plan estratégico institucional y éste con el Plan Nacional de Desarrollo y las políticas públicas de gobierno.

El plan informático estratégico tendrá un nivel de detalle suficiente para permitir la definición de planes operativos de tecnología de Información y especificará como ésta contribuirá a los objetivos estratégicos de la organización; incluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, se considerará la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario.

La unidad de tecnología de información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia. Dichos planes asegurarán que se asignen los recursos apropiados de la función de servicios de tecnología de información a base de lo establecido en su plan estratégico.

El plan estratégico y los planes operativos de tecnología de información, así como el presupuesto asociado a éstos serán analizados y aprobados por la máxima autoridad de la organización e incorporados al presupuesto anual de la organización; se actualizarán de manera permanente, además de ser monitoreados y evaluados en forma trimestral para determinar su grado de ejecución y tomar las medidas necesarias en caso de desviaciones.

410-04 Políticas y procedimientos

La máxima autoridad de la entidad aprobará las políticas y procedimientos que permitan organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria.

La unidad de tecnología de información definirá, documentará y difundirá las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización, estos se actualizarán permanentemente e incluirán las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran.

Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales

además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información.

Será necesario establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización.

Se incorporarán controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.

Se implantarán procedimientos de supervisión de las funciones de tecnología de información, ayudados de la revisión de indicadores de desempeño y se medirá el cumplimiento de las regulaciones y estándares definidos.

La unidad de tecnología de información deberá promover y establecer convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como de programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información.

410-05 Modelo de información organizacional

La unidad de tecnología de información definirá el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes.

El diseño del modelo de información que se defina deberá constar en un diccionario de datos corporativo que será actualizado y documentado de forma permanente, incluirá las reglas de validación y los controles de integridad y consistencia, con la identificación de los sistemas o módulos que lo conforman, sus relaciones y los objetivos estratégicos a los que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente.

Se deberá generar un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad.

410-06 Administración de proyectos tecnológicos

La unidad de tecnología de información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad. Los aspectos a considerar son:

1. Descripción de la naturaleza, objetivos y alcance del proyecto, su relación con otros proyectos institucionales, sobre la base del compromiso, participación y aceptación de los usuarios interesados.
2. Cronograma de actividades que facilite la ejecución y monitoreo del proyecto que incluirá el talento humano (responsables), tecnológicos y financieros además de los planes de pruebas y de capacitación correspondientes.
3. La formulación de los proyectos considerará el Costo Total de Propiedad CTP; que incluya no sólo el costo de la compra, sino los costos directos e indirectos, los beneficios relacionados con la compra de equipos o programas informáticos,

aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios.

4. Para asegurar la ejecución del proyecto se definirá una estructura en la que se nombre un servidor responsable con capacidad de decisión y autoridad y administradores o líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades.
5. Se cubrirá, como mínimo las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante el uso de actas o documentos electrónicos legalizados.
6. El inicio de las etapas importantes del proyecto será aprobado de manera formal y comunicado a todos los interesados.
7. Se incorporará el análisis de riesgos. Los riesgos identificados serán permanentemente evaluados para retroalimentar el desarrollo del proyecto, además de ser registrados y considerados para la planificación de proyectos futuros.
8. Se deberá monitorear y ejercer el control permanente de los avances del proyecto.
9. Se establecerá un plan de control de cambios y un plan de aseguramiento de calidad que será aprobado por las partes interesadas.
10. El proceso de cierre incluirá la aceptación formal y pruebas que certifiquen la calidad y el cumplimiento de los objetivos planteados junto con los beneficios obtenidos.

410-07 Desarrollo y adquisición de software aplicativo

La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:

1. La adquisición de software o soluciones tecnológicas se realizarán sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo previamente aprobados considerando las políticas públicas establecidas por el Estado, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.
2. Adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de software, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.
3. Identificación, priorización, especificación y acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias. Esto incluye, tipos de usuarios, requerimientos de: entrada, definición de interfaces, archivo, procesamiento, salida, control, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en donde aplique.
4. Especificación de criterios de aceptación de los requerimientos que cubrirán la definición de las necesidades, su factibilidad tecnológica y económica, el análisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del software de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse.

5. En los procesos de desarrollo, mantenimiento o adquisición de software aplicativo se considerarán: estándares de desarrollo, de documentación y de calidad, el diseño lógico y físico de las aplicaciones, la inclusión apropiada de controles de aplicación diseñados para prevenir, detectar y corregir errores e irregularidades de procesamiento, de modo que éste, sea exacto, completo, oportuno, aprobado y auditable. Se considerarán mecanismos de autorización, integridad de la información, control de acceso, respaldos, diseño e implementación de pistas de auditoría y requerimientos de seguridad. La especificación del diseño considerará las arquitecturas tecnológicas y de información definidas dentro de la organización.
6. En caso de adquisición de programas de computación (paquetes de software) se preverán tanto en el proceso de compra como en los contratos respectivos, mecanismos que aseguren el cumplimiento satisfactorio de los requerimientos de la entidad. Los contratos tendrán el suficiente nivel de detalle en los aspectos técnicos relacionados, garantizar la obtención de las licencias de uso y/o servicios, definir los procedimientos para la recepción de productos y documentación en general, además de puntualizar la garantía formal de soporte, mantenimiento y actualización ofrecida por el proveedor.
7. En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor será de la entidad contratante y el contratista entregará el código fuente. En la definición de los derechos de autor se aplicarán las disposiciones de la Ley de Propiedad Intelectual. Las excepciones serán técnicamente documentadas y aprobadas por la máxima autoridad o su delegado.
8. La implementación de software aplicativo adquirido incluirá los procedimientos de configuración, aceptación y prueba personalizados e implantados. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema.
9. Los derechos de autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso.
10. Formalización con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción y su revisión en la post-implantación.
11. Elaboración de manuales técnicos, de instalación y configuración; así como de usuario, los cuales serán difundidos, publicados y actualizados de forma permanente.

410-08 Adquisiciones de infraestructura tecnológica

La unidad de tecnología de información definirá, justificará, implantará y actualizará la infraestructura tecnológica de la organización para lo cual se considerarán los siguientes aspectos:

1. Las adquisiciones tecnológicas estarán alineadas a los objetivos de la organización, principios de calidad de servicio, portafolios de proyectos y servicios, y constarán en el plan anual de contrataciones aprobado de la institución, caso contrario serán autorizadas por la máxima autoridad previa justificación técnica documentada.

2. La unidad de tecnología de información planificará el incremento de capacidades, evaluará los riesgos tecnológicos, los costos y la vida útil de la inversión para futuras actualizaciones, considerando los requerimientos de carga de trabajo, de almacenamiento, contingencias y ciclos de vida de los recursos tecnológicos. Un análisis de costo beneficio para el uso compartido de Data Center con otras entidades del sector público, podrá ser considerado para optimizar los recursos invertidos.
3. En la adquisición de hardware, los contratos respectivos, tendrán el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, unidades de entrada/salida, entre otros, y las garantías ofrecidas por el proveedor, a fin de determinar la correspondencia entre los equipos adquiridos y las especificaciones técnicas y requerimientos establecidos en las fases precontractual y contractual, lo que será confirmado en las respectivas actas de entrega/recepción.
4. Los contratos con proveedores de servicio incluirán las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad y confidencialidad de la información, además de los requisitos legales que sean aplicables. Se aclarará expresamente que la propiedad de los datos corresponde a la organización contratante.

410-09 Mantenimiento y control de la infraestructura tecnológica

La unidad de tecnología de información de cada organización definirá y regulará los procedimientos que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades. Los temas a considerar son:

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios.
2. Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios serán registrados, evaluados y autorizados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción. El detalle e información de estas modificaciones serán registrados en su correspondiente bitácora e informados a todos los actores y usuarios finales relacionados, adjuntando las respectivas evidencias.
3. Control y registro de las versiones del software que ingresa a producción.
4. Actualización de los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice, los mismos que estarán en constante difusión y publicación.
5. Se establecerán ambientes de desarrollo/pruebas y de producción independientes; se implementarán medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura.
6. Se elaborará un plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardware y software, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

7. Se mantendrá el control de los bienes informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables.
8. El mantenimiento de los bienes que se encuentren en garantía será proporcionado por el proveedor, sin costo adicional para la entidad.

410-10 Seguridad de tecnología de información

La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

1. Ubicación adecuada y control de acceso físico a la unidad de tecnología de información y en especial a las áreas de: servidores, desarrollo y bibliotecas;
2. Definición de procedimientos de obtención periódica de respaldos en función a un cronograma definido y aprobado;
3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;
4. Almacenamiento de respaldos con información crítica y/o sensible en lugares externos a la organización;
5. Implementación y administración de seguridades a nivel de software y hardware, que se realizará con monitoreo de seguridad, pruebas periódicas y acciones correctivas sobre las vulnerabilidades o incidentes de seguridad identificados.
6. Instalaciones físicas adecuadas que incluyan mecanismos, dispositivos y equipo especializado para monitorear y controlar fuego, mantener ambiente con temperatura y humedad relativa del aire contralado, disponer de energía acondicionada, esto es estabilizada y polarizada, entre otros;
7. Consideración y disposición de sitios de procesamiento alternativos.
8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana.

410-11 Plan de contingencias

Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

Los aspectos a considerar son:

1. Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.
2. Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.

3. Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.
4. Plan de recuperación de desastres que comprenderá:

- Actividades previas al desastre (bitácora de operaciones)
- Actividades durante el desastre (plan de emergencias, entrenamiento)
- Actividades después del desastre.

5. Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia.
6. El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.
7. El plan de contingencias aprobado, será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.

410-12 Administración de soporte de tecnología de información

La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.

Los aspectos a considerar son:

1. Revisiones periódicas para determinar si la capacidad y desempeño actual y futura de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios.
2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad.
3. Estandarización de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas.
4. Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.
5. Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos.
6. Definición y manejo de niveles de servicio y de operación para todos los procesos críticos de tecnología de información sobre la base de los requerimientos de los usuarios o clientes internos y externos de la entidad y a las capacidades tecnológicas.

7. Alineación de los servicios claves de tecnología de información con los requerimientos y las prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos.
8. Administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios que demandan los usuarios, a través de mecanismos efectivos y oportunos como mesas de ayuda o de servicios, entre otros.
9. Mantenimiento de un repositorio de diagramas y configuraciones de hardware y software actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción.
10. Administración adecuada de la información, librerías de software, respaldos y recuperación de datos.
11. Incorporación de mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación.

410-13 Monitoreo y evaluación de los procesos y servicios

Es necesario establecer un marco de trabajo de monitoreo y definir el alcance, la metodología y el proceso a seguir para monitorear la contribución y el impacto de tecnología de información en la entidad.

La unidad de tecnología de información definirá sobre la base de las operaciones de la entidad, indicadores de desempeño y métricas del proceso para monitorear la gestión y tomar los correctivos que se requieran.

La unidad de tecnología de información definirá y ejecutará procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios recibidos.

La unidad de tecnología de información presentará informes periódicos de gestión a la alta dirección, para que ésta supervise el cumplimiento de los objetivos planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño.

410-14 Sitio web, servicios de internet e intranet

Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos.

La unidad de tecnología de información considerará el desarrollo de aplicaciones web y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general.

410-15 Capacitación informática

Las necesidades de capacitación serán identificadas tanto para el personal de tecnología de información como para los usuarios que utilizan los servicios de información, las cuales constarán en un plan de capacitación informático, formulado conjuntamente con

la unidad de talento humano. El plan estará orientado a los puestos de trabajo y a las necesidades de conocimiento específicas determinadas en la evaluación de desempeño e institucionales.

410-16 Comité informático

Para la creación de un comité informático institucional, se considerarán los siguientes aspectos:

- El tamaño y complejidad de la entidad y su interrelación con entidades adscritas.
- La definición clara de los objetivos que persigue la creación de un comité de informática, como un órgano de decisión, consultivo y de gestión que tiene como propósito fundamental definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos, así como apoyar en esta materia a las unidades administrativas que conforman la entidad.
- La conformación y funciones del comité, su reglamentación, la creación de grupos de trabajo, la definición de las atribuciones y responsabilidades de los miembros del comité, entre otros aspectos.

410-17 Firmas electrónicas

Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento.

El uso de la firma electrónica en la administración pública se sujetará a las garantías, reconocimiento, efectos y validez señalados en estas disposiciones legales y su normativa secundaria de aplicación.

Las servidoras y servidores autorizados por las instituciones del sector público podrán utilizar la firma electrónica contenida en un mensaje de datos para el ejercicio y cumplimiento de las funciones inherentes al cargo público que ocupan.

Los aplicativos que incluyan firma electrónica dispondrán de mecanismos y reportes que faciliten una auditoría de los mensajes de datos firmados electrónicamente.

a) Verificación de autenticidad de la firma electrónica

Es responsabilidad de las servidoras y servidores de las entidades o dependencias del sector público verificar mediante procesos automatizados de validación, que el certificado de la firma electrónica recibida sea emitido por una entidad de certificación de información acreditada y que el mismo se encuentre vigente.

b) Coordinación interinstitucional de formatos para uso de la firma electrónica

Con el propósito de que exista uniformidad y compatibilidad en el uso de la firma electrónica, las entidades del sector público sujetos a este ordenamiento coordinarán y definirán los formatos y tipos de archivo digitales que serán aplicables para facilitar su utilización. Las instituciones públicas adoptarán y aplicar los estándares

tecnológicos para firmas electrónicas que las entidades oficiales promulguen, conforme a sus competencias y ámbitos de acción.

c) Conservación de archivos electrónicos

Los archivos electrónicos o mensajes de datos firmados electrónicamente se conservarán en su estado original en medios electrónicos seguros, bajo la responsabilidad del usuario y de la entidad que los generó. Para ello se establecerán políticas internas de manejo y archivo de información digital.

d) Actualización de datos de los certificados de firmas electrónicas

Las servidoras y servidores de las entidades, organismos y dependencias del sector público titulares de un certificado notificarán a la entidad de certificación de Información sobre cualquier cambio, modificación o variación de los datos que constan en la información proporcionada para la emisión del certificado. Cuando un servidor público deje de prestar sus servicios temporal o definitivamente y cuente con un certificado de firma electrónica en virtud de sus funciones, solicitará a la entidad de certificación de información, la revocación del mismo, además, el superior jerárquico ordenará su cancelación inmediata. El dispositivo portable seguro será considerado un bien de la entidad o dependencia pública y por tanto, a la cesación del servidor, será devuelto con la correspondiente acta de entrega recepción.

e) Seguridad de los certificados y dispositivos portables seguros

Los titulares de certificados de firma electrónica y dispositivos portables seguros serán responsables de su buen uso y protección. Las respectivas claves de acceso no serán divulgadas ni compartidas en ningún momento. El servidor solicitará la revocación de su certificado de firma electrónica cuando se presentare cualquier circunstancia que pueda comprometer su utilización.

f) Renovación del certificado de firma electrónica

El usuario solicitará la renovación del certificado de firma electrónica con la debida anticipación, para asegurar la vigencia y validez del certificado y de las actuaciones relacionadas con su uso.

g) Capacitación en el uso de las firmas electrónicas

La entidad de certificación capacitará, advertirá e informará a los solicitantes y usuarios de los servicios de certificación de información y servicios relacionados con la firma electrónica, respecto de las medidas de seguridad, condiciones, alcances, limitaciones y responsabilidades que deben observar en el uso de los servicios contratados. Esta capacitación facilitará la comprensión y utilización de las firmas electrónicas, en los términos que establecen las disposiciones legales vigentes.